Miika Lippojoki

VERKON ANALYSOINTIOHJELMAT VERKONHALLINNASSA

Opinnäyte
Kajaanin ammattikorkeakoulu
Tradenomikoulutus
Syksy 2005

SISÄLLYS

TIIVISTELMÄ

ABSTRACT

SYMBOLILUETTELO

1 JOHDANTO 1
2 VERKONVALVONTA OSANA VERKONHALLINTAA 2
2.1 Vikojen hallinta 2
2.2 Käytön hallinta 3
2.3 Kokoonpanon hallinta 3
2.4 Suorituskyvyn hallinta 3
2.5 Turvallisuuden hallinta 4
2.6 Verkkoliikenteen tarkkailu 4
2.7 Verkonvalvontatyökalujen tarkoitus 6
3 VERKONVALVONTAOHJELMIEN TOIMINTAPERIAATE 7
3.1 Hallintalaite 7
3.2 Agentti 7
3.3 Tiedonvaihdon protokolla 8
3.4 Toimintaperiaate 8
3.5 SNMP, MIB JA RMON 11
3.5.1 SNMP 11
3.5.2 MIB 13
3.5.3 RMON 14
3.6 PERUSTYÖKALUJA VERKON TARKKAILUUN 16
3.6.1 Ping 16
3.6.2 Traceroute 17
4 ANALYSOINTIOHJELMIEN VERTAILU 18
4.1 Testausympäristö 18
4.2 Fluke Networks Network Inspector Console ja Protocol Inspector 20
4.2.1 Hälytykset 21
4.2.2 Datapaketit 22
4.2.3 Tilastot ja raportit 23

4.3 Commview 5.0 25
4.3.1 Hälytykset 26
4.3.2 Säännöt 28
4.3.3 Datapaketit 29
4.3.4 Tilastot 31
4.4 PRTG Traffic Grapher 32
4.5 YHTEENVETO 33
5 POHDINTA 36
LÄHTEET 38

Kajaanin ammattikorkeakoulu

OPINNÄYTETYÖ
TIIVISTELMÄ

Ala	Koulutusohjelma
Luonnontieteiden ala	Tietojenkäsittely
Tekijä(t): Miika Lippojoki	
Työn nimi: Verkon analysointiohjelmat verkonhallinnassa	
Vaihtoehtoiset ammattiopinnot: Järjestelmän ylläpito	Ohjaaja(t): Veli-Pekka Piirainen
Aika: 24.11.2005	Sivumäärä: 37 + 1

Tiivistelmä

Tämän opinnäytetyön aiheena oli tutustua verkon analysointiohjelmiin ja vertailla ilmaisohjelmia maksullisiin versioihin. Vertailun avulla pyritään kartoittamaan ohjelmien ominaisuuksien ja käyttömahdollisuuksien eroja. Työ tehtiin Kajaanin ammattikorkeakoululle.

Opinnäytetyössä perehdyttiin verkon analysointiohjelmien toimintaan ja pohdittiin kuinka analysointiohjelmat ovat avuksi verkonhallinnassa. Myös analysointiohjelmien yleisimpiä ominaisuuksia tutkittiin työssä. Lisäksi tutustuttiin verkonvalvonnassa käytettävien protokollien ja tietokantojen toimintaan.

Analysointiohjelmien vertailussa keskityttiin tarkkailemaan eri ohjelmien toimintaa verkonvalvonnassa. Jokainen kolmesta ohjelmasta testattiin testiympäristössä ja tämän jälkeen vertailtiin saatuja tuloksia toisiinsa. Yksi ohjelmista on käytössä Kajaanin ammattikorkeakoulussa ja tämän vertailun tarkoituksena oli kartoittaa heidän ohjelmansa ominaisuuksia verkonvalvonnassa.

Analysointiohjelmien ominaisuuksien vaihtelevuus on huomattava. Toiminnaltaan ohjelmat näyttävät muistuttavan huomattavasti toisiaan, mutta kaapatun datan tutkiminen ja erilaiset tilastot vaihtelevat ohjelmakohtaisesti huomattavasti. Analysointiohjelmien vertailu onnistui tässä opinnäytetyössä vaaditulla tavalla ja testaustuloksissa eroavaisuuksia saatiin aikaan.

Luottamuksellisuus	julkinen
Hakusanat	verkon analysointi, SNMP, verkonhallinta
Säilytyspaikka	Kajaanin ammattikorkeakoulun kirjasto

Kajaanin ammattikorkeakoulu

ABSTRACT OF THESIS

School Business	Degree programme Data Processing
Author(s) Miika Lippojoki	
Title Assistance of Network Analysis Programs in Network Management	
Alternative professional studies System support	Instructor(s) Veli-Pekka Piirainen
Date 24 November 2005	Total number of pages 37+1

Abstract

The purpose of this study was to gather information about network analysis programs and to compare free analysis programs with chargeable versions. Program comparison was helpful when finding out features and usage possibilities of the programs. The study was commissioned by the Kajaani Polytehcnic.

The main idea in this work was to examine how network analysis programs operate and how the programs could be of assistance in network management. The main features of the programs were also analysed, as well as the protocols and databases used in network management.

The comparison of the analysis programs was concetrated on the monitoring of the operations of all the tested programs. All the three programs were tested in a test environment and after that the results were compared. One of the programs is being used in the Kajaani Polytechnic and the purpose of the testing was to gather information about this program and compare the results with other similar programs.

Feature variety in different kinds of network analysis programs is considerable. Allthough the programs seem to be quite similar when operating, there are many differences in features like statistics and data capturing. The comparison of the analysis programs succeeded as specified in this study and differences could be found between analysis programs through the test results.

Confidentiality status	public
Keywords	Network Analysis, SNMP, Network Management
Deposited at	Kajaani Polytechnic Library

SYMBOLILUETTELO

ASN.1	Abstract Syntax Notation One käyttöjärjestelmä- ja ohjelmointikieliriippumaton tietorakenteiden määrittelyyn käytetty kuvauskieli
ICMP	Internet Control Message Protocol kontrolliprotokolla, jolla lähetetään nopeasti viestejä koneesta toiseen tavallisen IP-liikenteen ohitse
MIB	Management Information Base SNMP:n hallittava tietokanta
RMON	Remote Monitoring Verkon etävalvontastandardi
SMI	Structure of Management Information verkonhallinta-protokolla
SNMP	Simple Network Management Protocol verkon analysointiohjelmien käyttämä tiedonsiirtoprotokolla
TCP/IP	Transfer Control Protocol/Internet Protocol yhteisnimitys internetissä käytettäville tietoliikenneprotokollille

1 JOHDANTO

Tietoliikenneverkkojen kehittyessä joudutaan kiinnittämään yhä enemmän huomiota tietoturvallisuuteen ja verkkojen yleiseen suojaukseen. Palomuurien ja virustorjuntaohjelmien avulla pystytään varsin tehokkaasti suojautumaan ulkopuolisilta hyökkäyksiltä ja tietovuodoilta.

Suurten organisaatioiden apuna on monien vuosien ajan ollut erilaisia verkonvalvontaohjelmistoja. Ohjelmien avulla pystytään tarkkailemaan ja tarpeen vaatiessa tutkimaan verkossa liikkuvaa dataa ja analysoimaan verkon rasitusastetta. Hyvin laaditun verkkoanalyysin avulla pystytään parantamaan verkon toimivuutta ja etsimään mahdolliset verkon pullonkaulat, jotka hidastavat verkon toimintaa.

Verkon analysointi- ja valvontaohjelmat ovat pääasiallisesti suunniteltu avuksi järjestelmänvalvojien päivittäisten työtehtävien hoitoon. Erilaiset raportit ja hälytykset tukevat toimia verkon paremman toiminnan takaamiseksi ja tämä edesauttaa verkonhallintaa ja parantaa verkon turvallisuutta.

Tässä opinnäytetyössä käydään läpi, mitä verkonvalvonta ja siihen käytettävät ohjelmat ovat sekä selvitetään yleisiä verkonvalvontatyökalujen ominaisuuksia ja toimintaperiaatteita. Lisäksi tutustutaan Fluke Networksin verkonvalvontaohjelmistoon, sen toimintaan verkkoliikenteen tarkkailussa ja vertaillaan ohjelmistoa kahteen muuhun verkonvalvontaohjelmaan. Vertailussa keskitytään pääasiallisesti ominaisuuksien eroavaisuuksiin.

2 VERKONVALVONTA OSANA VERKONHALLINTAA

Kaikkein tärkeimmät järjestelmänvalvojan työkalut ovat nykyään ohjelmistoja laitteistojen sijaan. Avuksi kasvavien ja monimutkaisten tietoverkkojen hallintaan on kehitetty ohjelmistoja, joilla voidaan kerätä tietoja ilman erillistä erikoislaitetta. (The TCP/IP Guide. 2005.)

Verkonhallinta jakautuu perinteisesti viiteen osaan: vikojen, käytön, kokoonpanojen, suorituskyvyn sekä turvallisuuden hallintaan. Lisäksi verkon tarkkailu on korostunut tämän päivän suurien lähiverkkojen järjestelmävalvojien toiminnan osana. Aktiivinen verkonvalvonta eli verkon tarkkailu tarkoittaa laitteiden tilan ja kuormituksen seurantaa, niille määriteltäviä hälytysrajoja sekä niistä saataviin hälytyksiin reagoimista sovitulla tavalla. (The TCP/IP Guide. 2005.)

2.1 Vikojen hallinta

Monimutkaisen verkon toiminnan varmistamiseksi on pidettävä huolta siitä, että järjestelmä kokonaisuutena ja jokainen olennainen laite on toimintakunnossa. Kun mahdollisia vikoja havaitaan, on ensimmäisenä paikallistettava täsmällisesti, missä vika on. Seuraavaksi eristetään muu verkko vian aiheuttamilta häiriöiltä. Tämän jälkeen verkko on konfiguroitava tai muutettava siten, että vian vaikutukset verkon toimintaan ovat minimaaliset ilman vikaantunutta komponenttia. Lopuksi korjataan tai vaihdetaan vikaantunut komponentti ja verkko palautetaan alkuperäiseen tilaansa. (Niininen, K. 1997.)

2.2 Käytön hallinta

Käytön hallintaan kuuluu verkon käytöstä johtuvien kulujen laskutus verkkoa käyttäviltä asiakkailta. Käytön hallintaan on myös verkon eri käyttöpisteiden liikennemittaukset ja niiden pohjalta arvioidaan käyttökustannukset sekä mahdollisesti voidaan neuvoa käyttäjiä käyttämään verkkoa tehokkaammin hyväkseen. Käytön hallinnassa verkonvalvonnalla saavutetaan hyötyä, mikäli verkkoa on tarkasteltu ja analysoitu niin, että on saatu selvitettyä kuinka verkon käyttöä voitaisiin entisestään tehostaa tai parantaa. (Niininen, K. 1997.)

2.3 Kokoonpanon hallinta

Nykyaikaiset tietoliikenneverkot koostuvat yksittäisistä laitteista ja alijärjestelmistä, jotka voidaan määritellä tekemään erilaisia toimintoja. Tietokone voidaan esimerkiksi konfiguroida toimimaan reitittimenä tai tavallisena tietokoneena, tai se voi suorittaa molempia tehtäviä. Kokoonpanon hallinnan tehtävänä on alustaa verkko sekä hallitusti ajaa alas koko verkko tai osa siitä. Sen tehtäviin kuuluu myös ylläpitää, lisätä ja päivittää laitteiden välisiä riippuvuuksia ja itse laitteiden tilaa koskevia tietoja verkon normaalissa käytössä. Verkonvalvonnan ja analysointiohjelmien avulla kokoonpanojen hallinnassa saatava hyöty toteutuu lähinnä laitekarttojen ja osoitelistausten avulla. Analysointiohjelmien avulla saadaan selville mahdolliset verkon alasajon aikana tapahtuneet hälytykset tai listattua laitteet, jotka eivät uudelleenkäynnistyksessä toimineet niin kuin olisi haluttu. (Niininen, K. 1997.)

2.4 Suorituskyvyn hallinta

Tietoliikenneverkon suorituskyvyn hallinta koostuu kahdesta laajasta toiminnosta, valvonnasta ja hallinnasta. Valvonta tarkoittaa verkon liikenteen tarkkailua, ja hallinta mahdollistaa suorituskyvyn tehostamisen tarjoamalla välineet verkon asetusten säätämiseen. Jälkimmäinen toiminto on hieman samankaltainen kokoonpanon hallinnan kanssa, mutta siihen kuuluvat tehtävät ovat tarkempia kuin varsinainen kokoonpanon hallinta. Analysointiohjelmien suurin hyöty saadaan juuri suorituskyvyn hallinnassa. Analysointiohjelmien erilaiset testit ja tilastot mahdollistavat monitahoisen

verkon suorituskyvyn kartoittamisen ja mahdollisten parannuskeinojen esille tulemisen.

2.5 Turvallisuuden hallinta

Turvallisuuden hallinta on verkkoon ja siihen liitettyihin laitteisiin pääsyn seurantaa ja kontrollointia, sekä pääsyä siihen tietoon, jota on kerätty verkon laitteista osana verkonhallintaa. Erilaiset lokeihin kerätyt tiedot ovat tärkeä osa turvallisuuden hallintaa. Siksi turvallisuuden hallinta onkin suurelta osalta lokien keräämistä, tallennusta ja analysointia. Turvallisuuden hallinta osana verkonhallintaa ei siis tarkoita tietokonejärjestelmien sisäistä käyttäjien ja käyttäjäryhmien oikeuksien määrittelyä. Turvallisuuden hallinta keskittyy siihen kenellä, ja mistä on oikeus käyttää eri laitteita ja niistä saatavia palveluita. (Niininen, K. 1997.)

2.6 Verkkoliikenteen tarkkailu

Mahdollisimman tarkka kuva verkon tilasta saadaan, kun tarkkaillaan verkkoliikennettä verkon jokaisessa segmentissä. Liikennettä tarkkailemalla saadaan selville sekä toimimattomat verkon osat, että varoitukset mahdollisista tulevista vioista, jos liikenne tukkeutuu. Näin saadaan selville, mikä verkon osa toimii huonosti.

Verkon tarkkailua vaikeuttaa huomattavasti verkkosegmenttien määrä. Mikäli verkko koostuu useista eri reitittimien takana olevista lähiverkoista, tarvitaan useampia verkon tarkkailupisteitä. Yksi tietyssä segmentissä oleva verkon tarkkailulaite tai – ohjelma ei pysty keräämään tietoa toisesta segmentistä. Näin ollen täydellisen verkonvalvonnan takaamiseksi tarvitaan yksi verkon tarkkailulaite tai – ohjelma jokaiseen verkkosegmenttiin. (Scott M. Ballew. 1998. 189 – 190.)

Lähes kaikki verkon aktiivilaitteet pystyvät keräämään tietoa verkkoliikenteestä. Reitittimet ja kytkimet pitävät lokitiedostoa niiden läpi kulkevan datan määrästä, osa jopa jakaa tiedot luokkiin protokollakohtaisesti. Ongelmaksi muodostuu tietojen kokoaminen. Verkkoliikenteen tarkkailuohjelmien ja aktiivilaitteiden keräämiä tietoja ei pystytä yleensä

analysoimaan saman sovelluksen alla. Tämä vaikeuttaa verkkoliikenteestä kerättyjen tietojen analysointia huomattavasti.

Tietojen kokoamisen avain on SNMP (Simple Network Management Protocol). Se ei määritä, mitä tietoja laitteen tulee kerätä, mutta se edellyttää, että käytössä on standardin mukainen MIB (Management Information Base).

Useat verkon tarkkailuohjelmista käyttävät SNMP-protokollaa ja näin ollen pystyvät tarjoamaan useita tapoja tietojen analysointiin ja käsittelyyn. Usein ohjelmilla voidaan vain tutkia historiatietoja ja trendejä pitkän ajan kuluessa kerättyjen tietojen perusteella, mutta ei niinkään tutkia liikennettä ajan tasalla. **(**Scott M. Ballew. 1998. 191–193.)

Yksinkertaisimmillaan analysointiohjelma vertaa verkon liikennettä ennalta asetettuihin kynnysarvoihin ja antaa hälytyksen, jos jokin tunnusluku ylittää tai alittaa rajan. Tällä tavoin ei saada historiatietoihin perustuvia trendejä, joita hienoimmat analyysit tuottavat, mutta saadaan silti käyttökelpoinen kuva verkon sen hetkisestä tilasta.

On tärkeää miettiä, mitä kerätään ja kuinka usein. Ylimääräisten tietojen kerääminen suurista verkoista saattaa merkitä useiden gigatavujen luokkaa olevia määriä päivittäin. Koska useiden laitteiden kiintolevyt ovat kooltaan muutamia kymmeniä gigatavuja, on huolellisesti valittava tallennettavat tiedot, otettava näytteet harvemmin tai lakata keräämästä historiatietoja. Jos tietoja karsitaan liikaa, ei voida tehdä liikennettä koskevia analyysejä ja verkon valvonta rajoittuu näin vain asemien tavoitettavuuden testaamiseen.

Kun toimintavaihtoehtoja on paljon, riippuu ratkaisuvaihtoehto verkon laajuudesta, kuinka suuri on verkon toimimattomuudesta aiheutuva menetys ja mitä resursseja on käytettävissä. Tavoitettavuustarkkailu onnistuu yksinkertaisesti eikä kuluta resursseja. Tarvitaan vain isäntäkone ja pieni ohjelma. (Scott M. Ballew. 1998. 197 – 200.)

Reittien valvonta yhdistettynä tavoitettavuuden tarkkailuun toimii hyvin keksikokoisissa verkoissa, mutta pienissä verkoissa molempia ei tarvita. Laajemmissa verkoissa ohjelmat, joilla analysoidaan eri laitteilta kerättyjä

tietoja, saattavat käydä liian monimutkaisiksi ellei niiden käyttöä rajoiteta vain johonkin verkon osaan, esimerkiksi niihin jotka ovat alttiimpia häiriöille tai joiden vikaantumisesta on eniten haittaa.

Liikenteen valvonta on mittausmenetelmistä kaikkein eniten resursseja vaativaa. Tavallisesti se edellyttää erillistä valvonta-asemaa, joka kokoaa, tallentaa ja analysoi liikennetilastoja sekä esittää ne luettavassa muodossa. Siihen on myös liityttävä jokin menetelmä, jolla liikennettä koskevat tiedot kerätään verkon laitteilta tai ainakin tärkeimmiltä laitteilta. Koska tähän tarvitaan paljon resursseja, useimmissa pienissä verkoissa siitä saatava hyöty ei ole kaiken tämän arvoista. Jos kuitenkin verkon toimimattomuudesta aiheutuvat kulut ovat huomattavat, liikenteen tarkkailu on ainoa tapa havaita ongelmat ennen niiden syntymistä, kun niiden korjaaminen maksaa vähiten. Siten sen rajoitettu käyttäminen kannattaa sellaisissa verkon osissa, joiden vikaantumisesta on eniten haittaa. (Scott M. Ballew. 1998. 200 - 205.)

2.7 Verkonvalvontatyökalujen tarkoitus

Verkonvalvontatyökalujen tarkoitus on pääsääntöisesti helpottaa verkkolaitteita käsittelevien ihmisten työtä. Niiden avulla voidaan suorittaa erilaisia verkkoliikennemittauksia, mahdollisesti muuttaa tietoliikennelaitteiden asetuksia yhdeltä hallintatyöasemalta, tarkkailla verkon tilaa ja näin huomata vikatilanteet ennen kuin ne pääsevät muodostumaan liian vakaviksi.

Verkonvalvontatyökaluilla on yleensä mahdollista toteuttaa samanaikaisesti verkonvalvontaa, ylläpitoa ja virhetilanteiden korjaamista ilman että tarvitsee poistua työasemalta kovinkaan kauaksi. Verkonhallintatyökalun liikennemittauksilla voidaan taata verkon liikenteen sujuvuus siten, että asetetaan tiettyihin verkon paikkoihin pisteitä joita mitataan säännöllisin väliajoin. Jos näistä pisteistä tulee hälytyksiä, voidaan verkkoa joko laajentaa tai reitittää liikenne kulkemaan jotain toista kautta. Lisäksi erilaisten väärinkäytösten ja verkon käyttöasteen tarkkailu tulee helpommaksi.

3 VERKONVALVONTAOHJELMIEN TOIMINTAPERIAATE

Verkonvalvontaohjelmien toiminta vaihtelee eri sovellusten mukaan. Suurin osa ohjelmista käyttää avukseen SNMP-protokollaa kerätessään tietoa verkkoliikenteestä. Yleisin ja varsin yksinkertainen toimintamalli verkonvalvontaohjelmilla on hallintalaite/agentti-arkkitehtuuri. Seuraavaksi käsitellään tätä arkkitehtuuria käyttävien verkonvalvontaohjelmien toimintaperiaate ja tutustutaan niiden sijoittamiseen lähiverkon alueella.

3.1 Hallintalaite

Hallintalaite on jokin työasema verkossa, johon valvontaohjelmisto halutaan asettaa käyttöön. Työasema valvontaohjelmineen mahdollistaa haettujen tietojen ja saapuneiden tiedotteiden perusteella esimerkiksi koontiviestien muodostamisen, graafien piirtämisen ja verkon laitteiden reaaliaikaisen tilanäkymän esittämisen. Lisäksi hallintalaiteella voidaan kontrolloida mittaustulosten perusteella verkon tilaa reaaliajassa.

3.2 Agentti

Agentti on hallinnan kohteena oleva laite tai siihen asennettu ohjelma, joka vastaa hallintalaitteelta tuleviin kyselyihin. Agentin tehtävänä on kerätä tietoa sen verkkosegmentin alueelta, johon se on asennettu toimimaan. Kerätty tieto tallennetaan omaan hallintatietokantaan, josta hallintatyöasema voi noutaa kerätyn tietopaketin analysoitavaksi. Lisäksi agentti osaa lähettää ennalta

määrättyjen tapahtumien sattuessa ilmoituksen hallintatyöasemaan sekä vastata hallinta-aseman lähettämiin kyselyihin.

Agentti voi toimia myös tiedonvälittäjänä toisessa verkkosegmentissä olevalle agentille. Tämän toiminnon ideana on mahdollistaa eri standardien väliseen kommunikaatioon kykenemättömät ohjelman osat ymmärtämään toisiaan. Välittävä agentti muuntaa sisään tulevat viestit kohdeagentin ymmärtämään muotoon ja vastaukset taas takaisin hallinta-aseman ymmärtämään muotoon. Etenkin suurissa verkoissa voidaan hyödyntää hierarkiaa, jossa hallintaohjelma kommunikoi vain muutaman agentin kanssa, jotka keräävät tietoa muutamalta agentin alla sijaitsevalta verkon solmulta. Näin verkonhallinta kuormittaa verkkoa tasaisemmin. (Niininen, K. 1997.)

3.3 Tiedonvaihdon protokolla

Hallintalaitteiden ja agenttien välinen kommunikaatio tapahtuu yleisten kommunikaatioprotokollien, kuten TCP/IP, välityksellä. Tyypillinen verkonhallintaprotokolla koostuu rajatusta ryhmästä kommunikointiviestejä, joita voivat olla yksittäisen tiedon haku tai asetusten muuttamiseen tarkoitettu viesti.

3.4 Toimintaperiaate

Mahdollisimman tarkan verkkoliikenteen ja verkon eri laitteiden määrän ja laadun kartoittamisen takaamiseksi tulee agentteja olla verkon jokaisessa solmussa. Hallintalaite pystyy käsittelemään jokaisen agentin tiedot erikseen tai vain solmun kerrallaan tilanteen niin vaatiessa. Agentti on kuin mikä tahansa muu palvelu tietokoneen ollessa käynnissä. Kun agentti käynnistetään, se ryhtyy keräämään tietoa määritettyjen asetuksien mukaisesti. Tiedot tallentuvat tietokantaan, josta ne ovat poimittavissa hallintalaitteen (pääohjelman) analysoitavaksi.

Tietoja voidaan kerätä joko tietystä verkkotoiminnasta tai analysoitavaksi voidaan kelpuuttaa mikä tahansa verkon kautta tapahtuva toiminta. Yleensä agentit sijoitetaan verkon solmukohtien läheisyyteen ja näin ollen mahdollistetaan ulko- ja sisäverkon välisen liikenteen tehokas tarkkailu.

Sijoittamalla agentit verkon aktiivilaitteiden läheisyyteen, voidaan saada selville esimerkiksi ulkoisen tunkeutujan käyttämä IP-osoite tai mahdollinen laitteen tai verkon rasittuvuuden syy. (Niininen, K. 1997.)

Pääsääntö on, että hallintaohjelman ja agentin MIB-tietokantojen tulee olla täsmälleen samanlaiset. Agentti osaa vastaa seuraaviin neljään komentoon, joilla voidaan käsitellä MIB-tietokantaa:

get	lukee agentin MIB-tietokannasta yhden tiedon.
getnext	lukee agentin MIB-tietokannasta järjestyksessä seuraavan tiedon.
walk	lukee agentin MIB-tietokannasta kaikki tiedot tietystä alkukohdasta alkaen.
set	käskee agentin antamaan arvon konfiguroitavalle parametrille tai nollaamaan jonkin tiedon, esimerkiksi lähteneiden datapakettien laskurin.

Agentin toiminta riippuu verkonvalvojan tarpeista. Agentti voi toimia seuraavasti:

- Valvontaohjelmisto lähettää agentille pyyntöjä ja agentti vastaa niihin.
- Agentti palauttaa vastauksen tiettyyn osoitteeseen saatuaan get- tai getnext-komennon.
- agentti lähettää walk-komennolla useita vastauksia selatessaan MIB-tietokantaa alaspäin annetusta alkukohdasta.
- Agentti vastaanottaa set-komentoja valvontaohjelmistolta ja asettaa raja-arvoja verkon valvontaa varten.
- Agentti voi ilman pyyntöä esimerkiksi seurata, ylittyykö jokin set-komennolla asetettu raja-arvo. Kun agentti on havainnut rajan ylityksen, se lähettää sanoman valvontaohjelmistolle. Lähetetystä sanomasta käy ilmi raja-arvon ylittäneen kohteen IP-osoite, sekä mikä raja on ylittynyt.

- Agentti voi myös lähettää ennalta pyytämättä sanomia, mikäli se havaitsee jotain erityistä tapahtuvan. Tällaisia sanomia kutsutaan pyydyssanomiksi (trap messages), sillä ne syntyvät, kun agentin ”pyydykseen” jää jotain. (TCP/IP Trainer. 2005.)

Hallinta-aseman ja agentin välinen toiminta riippuu hallinta-asemassa olevista ohjelmista. Mikäli käytössä on komentorivipohjainen valvontaohjelma, kuten SNMPGet, tulee verkonvalvojan olla erittäin tietoinen MIB-tietokannan rakenteesta. Tällöin tulee tietää tarkkaan niin komennot kuin haettavien arvojen sijainnit MIB-tietokannassa, että agentin lähettämä vastausviesti olisi halutunlainen. Mikäli käytössä on graafisella käyttöliittymällä toteutettu valvontaohjelma, kuten Network Inspector Console, agentti kerää tiedot verkkoon kytketyistä laitteista ilman erillistä sanomien luomista.

Seuraavassa esimerkissä on tilanne, jossa hallinta-asema (komentorivipohjainen) haluaa tietää jostain laitteesta sen yhteyshenkilön, nimen ja sijainnin. Hallinta-asema lähettää agentille seuraavanlaisen get-viestin:

GetRequest (sysContact.0, sysName.0, sysLocation.0)

Mikäli käytettävässä hallinta-aseman ja agentin käyttämässä MIB-tietokannassa on sallittua näyttää tietoja yhteisön jäsenistä, lähettää agentti takaisin seuraavanlaisen Get-vastausviestin:

GetResponse ((sysContact.0 = Carlos), (sysName.0 = carlos.lnet.lut.fi), (sysLocation.0 = SK28))

Viestistä käy ilmi hallinta-aseman haluamat tiedot kyseisen laitteen osalta. Hallinta-aseman pääohjelma tulostaa mahdollisuuksien mukaan käyttöliittymään laitteen yhteyshenkilön, laitteen nimen sekä laitteen sijainnin verkossa.

3.5 SNMP, MIB JA RMON

3.5.1 SNMP

Internetin yleistyttyä ja siihen kytketyn laitekannan kasvettua rajusti syntyi tarve yleispäteville tavoille verkon hallintaan. SNMP suunniteltiin reitittimien ja verkon muiden laitteiden etäältä tapahtuvaa hallintaa varten yksinkertaista kyselyprotokollaa käyttämällä. SNMP:tä tuntevan laitteen hallinta ja valvonta tapahtuu siten, että verkonvalvonta-asemassa toimiva hallintaohjelma lähettää pyynnön agenttiohjelmalle joka toimii valvottavassa laitteessa. Pyyntö voi koskea laitteen asetusten muuttamista tai laitetta koskevien tietojen antamista.

Jokainen SNMP-laite ylläpitää tietokantaa nimeltä MIB (Management Information Base). se sisältää kaikki ne tiedot joita laite ylläpitää ja käyttää oman toimintansa ohjaamiseen. Laitetta valvotaan pyytämällä sitä lähettämään tässä tietokannassa olevia tietoja. MIB sisältää esimerkiksi tiedot siitä, montako oktettia on vastaanotettu jokaisesta liitännästä. Pyytämällä laitetta lähettämään nämä tiedot voidaan laskea kuinka monta oktettia laite on yhteensä vastaan ottanut sen jälkeen kun laskurit viimeksi nollattiin. SNMP-laitteen hallinta tapahtuu tallentamalla sen toimintaa ohjaavia asetuksia MIB-tietokantaan. (Cisco Ltd. 2005a.)

SNMP-hallintaohjelmisto voi olla vain yksinkertainen yleiskäyttöinen kyselyohjelma, jota käyttämällä verkonhallitsija voi noutaa tietoja MIB-tietokannasta tai se voi olla ohjelmisto joka toimii erityisessä automaattista valvontaa suorittavassa verkonhallinta-asemassa. Kun käytetään erillistä valvonta-asemaa, on mahdollista jopa aikatauluttaa asetusmuutokset lähetettäviksi automaattisesti yön aikana.

SNMP:n heikkous on, että suuri määrä tietoja on pidettävä tallennettuina eri laitteiden MIB-tietokantaan. SNMP:n tärkein seikka on ymmärtää, mitkä tiedot ovat käyttökelpoisia ja milloin. Jos ei aiota valvoa laitteen läpi kulkevaa liikennettä, liittymiä koskevat laskurit eivät ole mielenkiintoisia. SNMP:n käyttäminen on yksinkertaisempaa, jos käytössä on verkonhallinta-asema jossa on hyvät työkaluohjelmat. Tällaisten työkalujen avulla voidaan tutkia

koko verkko ja muodostaa siitä topologinen kartta, jossa voidaan esittää tarpeellinen määrä yksityiskohtia ja hälytykset esimerkiksi eri värein. Ne sisältävät mahdollisesti myös valmiit toimintosarjat, jotka keräävät kaikista liittymistä niiden osoitetiedot ja liikennetiedot sekä esittävät ne helposti luettavassa muodossa. Tällaiset toimintosarjat SNMP:n perustoimintoja käyttämällä saattaisivat vaatia satoja kyselyitä ja vastauksia, jotka olisi tulkittava ja esitettävä. (Cisco Ltd. 2005a.)

SNMP-verkonhallinta-aseman todellinen vahvuus on siinä, että sillä pystytään hallitsemaan eri valmistajien erilaisia laitteita vain yhtä käyttöliittymää ja samoja työkaluja käyttäen. Näin ollen ei tarvita useita erilaisia ohjelmia ja komentoja, että saataisiin selville verkossa olevien laitteiden tietoja.

Alkuperäinen SNMP-protokollaperhe koostuu kolmesta pääosasta. Ne ovat itse protokolla, tietorakenteiden määrittelyt sekä näihin liittyvät kokonaisuudet, joilla käytettävä tietokanta määritellään.

SNMP:n kantavana ideana on yksinkertaisuus. Yksinkertaisuuteen pyritään hyvin rajatuilla kommunikointifunktioilla eli viesteillä ja viestien käyttämisestä aiheutuvalla pienellä verkkokuormalla. SNMP on standardisoitu avoin verkonhallintaprotokolla, joten sen kehityksestä ei huolehdi pelkästään standardisointikomiteat, vaan kehitykseen voi osallistua koko Internet-yhteisö. SNMP:n suurta suosiota pitää yllä kattava tuki suurimmilta verkkokomponenttien valmistajilta. Kaikki SNMP-yhteensopivat laitteet tarjoavat samanlaisen liittymän verkonhallinta-asemalle, mikä lisää yhteensopivuutta ja vähentää suunnittelun määrää tuotekehityksessä. SNMP on protokollana käyttöjärjestelmä- ja ohjelmointikieliriippumaton. SNMP:n ideologiaan kuuluu kevyt toteutus, jonka vaikutus olisi nimellinen suoritusympäristön muuhun toimintaan nähden. (Cisco Ltd. 2005a.)

SNMP on hyödyllinen, mutta siinä on puutteita. Valvontaohjelmiston ja agentin pyyntöihin perustuva kommunikointi aiheuttaa paljon liikennettä verkkoon ja näin kuormittaa sitä. Lisäksi SNMP ei varoita ennalta ilmaantuvista ongelmista ennen kuin niistä tulee vakavia, vaikka se poikkeuksellisista tapahtumista

ilmoittaakin. SNMP saa MIB-tietokannan avulla selville tiettyjen laitteiden tapahtumat, mutta tärkein puute on, ettei se pysty kertomaan, kuinka kokonainen verkkosegmentti käyttäytyy. (TCP/IP Trainer. 2005.)

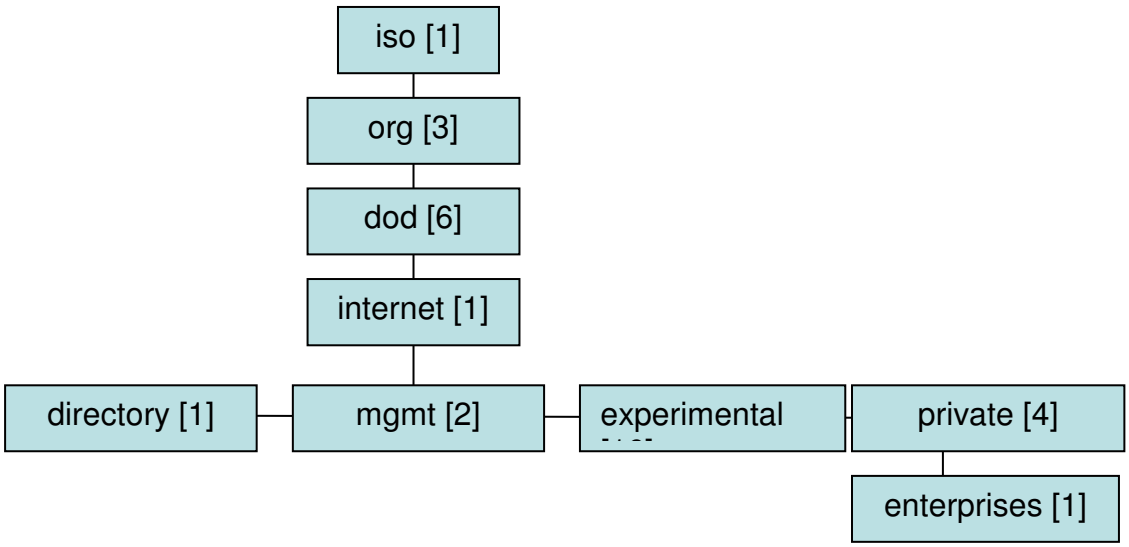
3.5.2 MIB

Kuten missä tahansa tiedonkeräyksessä, niin myös verkonvalvonnassa koko järjestelmän perusta rakentuu tietokannan päälle. SNMP:n hallittavan tietokannan nimi on MIB. Jokaista hallittavaa tai tarkkailtavaa kohdetta (esimerkiksi portti tai hälytysasetukset) nimitetään objektiksi. Looginen rakenne MIB-tietokannalle on puumallinen ja tämä on myös se näkymä, joka SNMP-agentin on tarjottava hallintaohjelmistolle. Käytännössä SNMP:n standardit eivät määrää kuinka kyseinen tietokanta toteutetaan fyysisesti laitteissa, joten laitevalmistajat voivat toteuttaa MIB-tietokannan rakenteen sisäisesti esim. relaatiotietokantana. MIB on tietokanta, joka sisältää SNMP-tiedonvaihdossa tarvittavan rakennekuvauksen, koska se koskee tiettyjä osoitteella varustettuja verkon komponentteja tai kohtia. MIB mahdollistaa valvontaohjelmiston ja agenttien välisen täsmällisen ja yksiselitteisen viestinnän. MIB muistuttaa DNS-rakennetta, joka on hierarkkinen ja joka käyttää pisteellistä kuvaustapaa osoitteissaan. (TCP/IP Trainer. 2005.)

Useimmat MIB-rakenteen kohteet tarkoittavat numeerisen arvon sisältäviä laskureita. Loput tiedoista voivat olla esimerkiksi tekstitietoina tai IP-osoitteina. Ne ovat asetustietoja joko verkonvalvontaa tai SNMP-protokollaa varten. MIB-rakennetta tutkitaan juuresta alkaen siihen asti, kunnes komento täysin vastaa haluttua tietoa.

MIB:n rakenteissa käytetään ASN.1 (Abstract Syntax Notation One) kuvauskieltä. Hallittavia resursseja kuvataan olioina, jotka ovat agentin tiettyjä ominaisuuksia kuvaavia muuttujia. Muuttujat on standardoitu niin, että kaikki samantyyppiset laitteet tukevat samaa joukkoa olioita. Olion nimi koostuu kokonaisluvuista, jotka erotellaan toisistaan pisteillä. MIB-tietotyyppien esitys- ja nimeämiskäytäntöjä varten kehitettiin määritelmä SMI (Structure of Management Information). Koska MIB-tietokanta on puunmuotoinen, ovat hallittavat oliot puun lehtinä ja jokainen haara kuvaa

olioiden ryhmittelyä toiminnan tai nimeämistä hallitsevan organisaation mukaan. Olioiden tunnisteet ovat niin kuin puhelinnumerot eli ne ovat järjestyksessä ja jokaiselle organisaatiolle on oma numeronsa. Suurin osa MIB-määrityksistä sijoittuu oliotunnisteen 1.3.6.1 alle, joka on tarkoitettu internet yhteisölle (Kuvio 1.).



Kuvio 1. MIB-hierarkian perusrakenne

Tämän yksinkertaistuksen ideana on parantaa eri järjestelmien yhteistoiminnallisuutta. Jokainen objekti MIB-tietokannassa on määritelty kaavamaisesti. Tämä tarkoittaa sitä, että jokaiselle objektille on tarkasti määritelty sen tyyppi, sen sallitut muodot, arvoavaruus ja sen suhde muihin MIB- objekteihin.

3.5.3 RMON

Tärkein lisäys perus-SNMP:n standardeihin on etähallintastandardi RMON (Remote Network-Monitoring), joka on MIB-osoiteavaruuden laajennus. Se kehitettiin verkon etäpisteiden ja paikallisverkkojen seurantaan ja ylläpitoon. Kun SNMP hakee tietoja yhdeltä tietokoneelta kerrallaan, pystyy RMON kaappaamaan tietoja suoraan verkkomediasta ja näin ollen se voi antaa tietoja myös paikallisverkon kokonaistoiminnasta. (TCP/IP Trainer. 2005.)

RMON-standardi määrittelee joukon tilastoja, toimintoja ja hälytyksiä, joita voidaan vaihtaa RMON-yhteensopivan konsolihallintaohjelman ja verkkoanalysaattorin välillä. RMON mahdollistaa näin järjestelmänvalvojan tarkan verkkovirhediagnosoinnin, verkonsuunnittelun ja verkon suorituskyvyn parantamisen saatavilla olevien tietojen avulla. (Cisco Ltd. 2005b.)

RMON kerää tilastotietoja verkon toiminnasta tiettyjen tietoryhmien mukaisesti. Periaatteessa puhutaan etähallittavasta MIB-tietokannasta, MIB-2:sta, joka sisältää tavallista MIB-tietokantaa laajemman määrän saataville asetettua tietoa laitteesta ja mahdollisista yhteisöistä, joihin laite kuuluu. Kukin RMON-ryhmä on siis MIB-2-tietokannan objekti. Näiden erityyppistä tietoa sisältävien ryhmien nimet ja tehtävät ovat:

Statistics	Tämä ryhmä sisältää tilastotietoja jokaisesta tutkittavasta verkkosegmentistä.
History	Tässä ryhmässä sijaitsevat tilastotiedot, joita päivitetään säännöllisesti ja jotka tallennetaan myöhempää käyttöä varten.
Alarm	Ryhmä tutkii agenttiin asetettuja arvoja säännöllisin otoksin ja vertaa arvoja annettuihin raja-arvoihin. Mikäli arvot ylittyvät, lähetetään ilmoitus valvontaohjelmistolle.
Host	Tässä ryhmässä pidetään tilastotietoja jokaisesta verkkosegmentin isäntäkoneesta analysoimalla datapakettien lähetys- ja vastaanotto-osoitteita.
Host Top N	Tämä ryhmä muodostaa raportteja isäntäkoneista, jotka ovat joissakin mittarien mittauksissa kärkisijoilla. Tällaisia mittauksia voivat olla esimerkiksi useimmiten ilmenevien koneiden osoitteiden kerääminen.

Matrix	Tässä ryhmässä ovat yhteystaulukot, joista ilmenee koneiden välillä lähetettyjen datapakettien määrät.
Filter	Tämän ryhmän kautta voidaan määrittää suodattimet, joilla tiettyjä datapaketteja suodatetaan verkkoliikenteestä.
Capture	Tällä tietoryhmällä saadaan filter-ryhmän suodatuksen läpäisseet datapaketit tallennetuksi myöhempää tarkastelua varten.
Event	Tämä tietoryhmä toimii Alarm-ryhmän kanssa. Se luo tapahtumia, joilla raja-arvojen ylityksistä ilmoitetaan verkonvalvojalle. (TCP/IP Trainer. 2005.)

3.6 PERUSTYÖKALUJA VERKON TARKKAILUUN

3.6.1 Ping

Yksinkertaisin ohjelma verkon toimivuuden tarkkailuun on ping-komento, joka kuuluu TCP/IP:tä käyttävän käyttöjärjestelmän perusohjelmiin. Se on käytettävissä niin henkilökohtaisissa työasemissa kuin suuritehoissa supertietokoneissa. Ping lähettää määritetylle asemalle ICMP echo-sanoman. Jokaisen IP-laitteen tulee vastata ICMP echo – sanomaan vastaussanomalla. Ping mittaa lähetyksen ja vastaanoton välisen ajan ja pystyy siten raportoimaan sekä tavoittavuuden että edestakaiseen matkaan kuluvan ajan.

Ping on ehkä kaikkein eniten verkon valvonnassa ja vikaselvityksessä käytetty työkalu, koska se on niin laajasti käytettävissä. Toisaalta sen tuottamat tiedot ovat vähäiset ja ne saattavat olla jopa harhaanjohtavia. Ensinnäkin lähtevä sanoma ja palautettu sanoma saattavat kulkea eri reittejä pitkin. Näin ollen puuttuva echo-vastaus ei kerro mikä monista mahdollisista reiteistä on vikaantunut. Se kertoo vain että et voi tavoittaa kohdetta ja saada vastausta. Lisäksi ICMP-echo-paketit ovat mahdollisesti poistettu datavirrasta ruuhkan vuoksi ja voivat jopa itsekin aiheuttaa ruuhkaa, koska ne ovat paketteja.

Kaikesta huolimatta ping tarjoaa nopean tavan tarkistaa tavoitettavuus ja se voi sellaisenaan luoda pohjan laajemmalle, mutta kuitenkin yksinkertaiselle tavoitettavuuden tarkistusjärjestelmälle. Se on usein ensimmäinen vikaselvityksessä käytettävä työkalu jolla voidaan esimerkiksi todeta ongelman laajuus. (Scott M. Ballew. 1998. 209–210.)

3.6.2 Traceroute

Traceroute on käyttökelpoinen silloin, kun kahden pisteen välissä on olemassa useampia reittivaihtoehtoja paketin perillepääsyn takaamiseksi. Traceroute jäljittää jokaisen reitittimen pisteiden A ja B välillä. näin ollen saadaan selville mikä siirtoteistä ei toimi tai mikä on lyhin mahdollinen reitti tiedon perille saattamiseksi.

.

4 ANALYSOINTIOHJELMIEN VERTAILU

Opinnäytetyön käytännön osio koostui Kajaanin ammattikorkeakoululla käytössä olevan verkon analysointiohjelman ominaisuuksien kartoituksesta ja niiden vertailusta saatavilla oleviin niin ilmaisiin kuin maksullisiin ohjelmiin. Lähinnä pyrittiin etsimään mahdollisia eroavaisuuksia ohjelmien toiminnassa niiden tutkiessa verkkoa.

Aluksi Internetistä etsittiin vertailuun sopivia ohjelmia. Lopullisen valinnan koittaessa ohjelmia oli yhteensä viisi kappaletta, joista testaukseen valittiin kolme. Vertailussa olivat mukana Fluke Networks Network Inspector, PRTG Traffic Grapher ja Commview 5.0. Ohjelmat olivat ominaisuuksiltaan varsin samanlaisia ja näin ollen testitulokset olivat samankaltaisia. Ohjelmien toiminnan vertailu oli helppoa, sillä kaikista ohjelmista löytyi tarvittavat ominaisuudet vertailun suorittamiseksi.

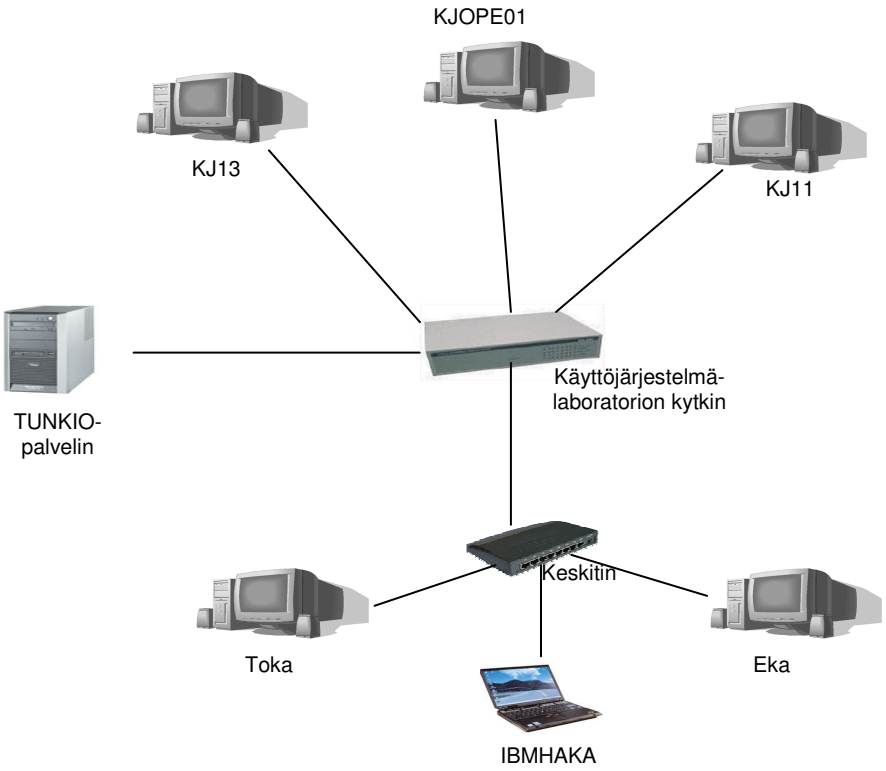
Vertailun alueiksi valittiin ominaisuuksista verkkoliikenteen kaappaus, laitetietojen keräys, verkossa tapahtuvien virheiden havainnointi sekä ohjelman yleinen käytettävyys ja toiminta. Nämä ovat yleisesti kaikkien verkon monitorointiohjelmien toimintoja, joten analysoinnista saatiin kattava ja riittävä kuva.

4.1 Testausympäristö

Verkkoliikenteen analysointia varten saatiin käyttöön Kajaanin ammattikorkeakoulun käyttöjärjestelmälaboratorio. Testattavat ohjelmistot

olivat asennettuina ammattikorkeakoululta lainassa olevassa kannettavassa tietokoneessa. Verkkoliikenteen simulointia varten asennettiin kahteen työasemaan Windows XP-käyttöjärjestelmä, sekä erilaisia tiedostoja siirreltäväksi koneiden kesken ja määritettiin verkkoyhteydet. Kannettava tietokone ja työasemat liitettiin työryhmään Testi ja ne pystyivät keskustelemaan keskenään kytkimen välityksellä.

Verkkoliikennettä kuvattiin internet-surffailulla, erilaisten datapakettien imuroinnilla ja datapakettien siirroilla koneesta toiseen. Verkkoliikennettä pyrittiin pitämään yllä mahdollisimman pitkään, että saataisiin hankittua pitkäaikaista tietoa verkon käytöstä ja näin ollen kerättyä mahdollista trenditietoa verkon käyttöasteesta. Tämä ei kuitenkaan onnistunut, koska käytössä ei ollut hallinnoitavaa kytkintä, joka olisi vaadittu trenditietojen keräykseen.



Kuvio 2. Testausympäristö.

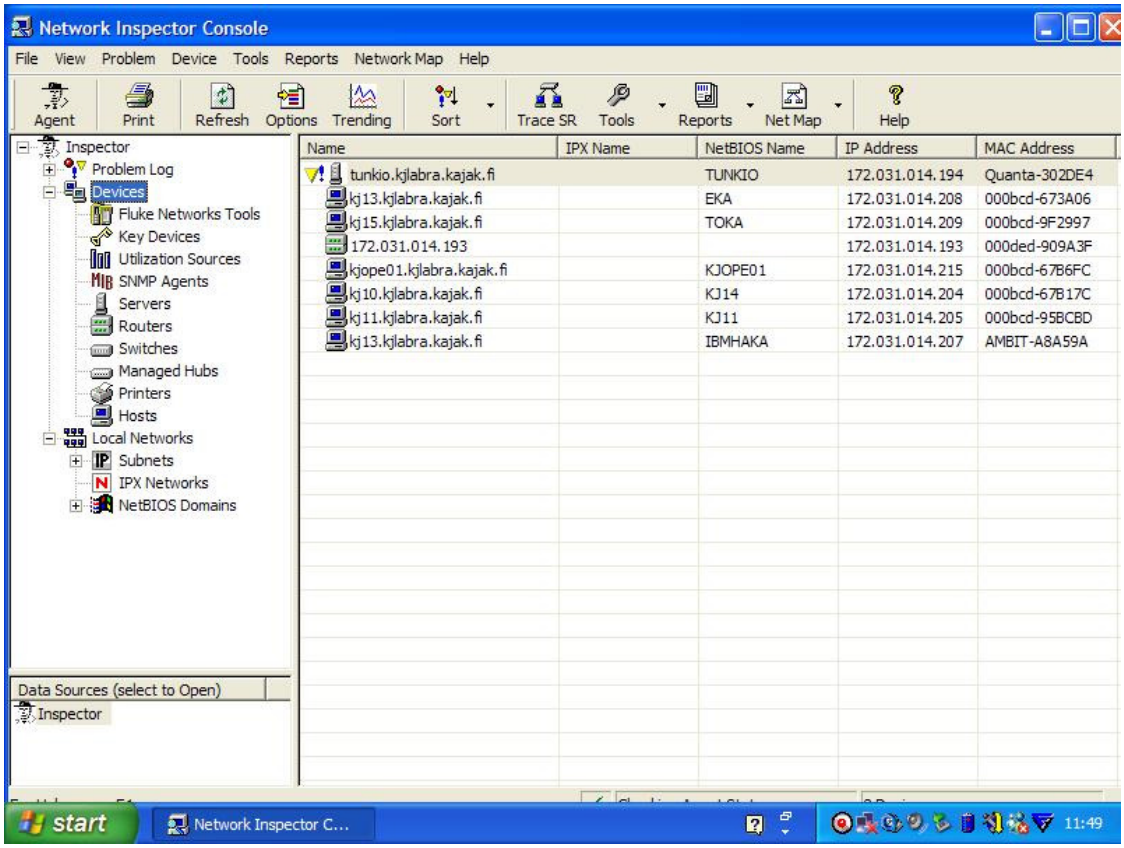
Testausympäristö laajeni, kun ainoana testattavista ohjelmista agentin sisältävä Network Inspector käynnistettiin, huomattiin, että agentti havaitsi myös laboratorion muut käynnissä olevat työasemat sekä laboratoriossa olevan palvelimen ja kytkinkaapissa olevan kytkimen (Kuvio 2.). Agentin työ rajautui kuitenkin laboratorion omaan lähiverkkoon, sillä agenttiohjelma ei pysty ilman erillistä määritystä tutkimaan laitteita kytkimen ulkopuolisesta verkosta.

4.2 Fluke Networks Network Inspector Console ja Protocol Inspector

Kajaanin ammattikorkeakoululla käytössä oleva analysointiohjelma osoittautui laajimmaksi ominaisuuksiltaan, mutta kaikkein hankalimmaksi hallinnaltaan. Ohjelma sopii erinomaisesti suuriin, oppilaitosverkkojen kaltaisiin ympäristöihin toimintansa puolesta. Network Inspector on lisäksi testatuista ohjelmista ainoa, jossa on erillinen hallintaohjelma ja agentti. Agentti oli asennettuna kannettavaan tietokoneeseen. Ohjelman etuina muihin verrattuina on juuri laajuus ja pikkutarkkuus verkonvalvonnan kannalta sekä muista ohjelmista puuttuva laitetietojen kerääminen pääikkunaan.

Laitetiedot pystyttiin keräämään testatuista ohjelmista tarkasti vain Network Inspectorin hallintaohjelman avulla. Inspector osaa jakaa laitteet niin tyypin kuin esimerkiksi aliverkkojen mukaiseen järjestykseen. Network Inspectorin laitetietojen esittäminen oli myös etevää, sillä se osaa jakaa laitteet mm. omien toimialueiden tai työryhmien mukaan sekä aktiivilaitteiden mukaan järjestykseen. Samoin Inspectorilla voidaan luoda IP-osoitelistoja, joissa näkyvät käynnissä olevien laitteiden nimet sekä osoitteet ja niiden tarjoamat palvelut (Kuvio 3.). Tämä helpottaa kytkettyinä olevien laitteiden kartoitusta sekä niiden sijainnin löytämistä. Itse pääohjelman avulla pystytään lisäksi luomaan verkon ns. trenditilastoa, josta nähdään ajallisesti verkon rasittuvuusasteiden huiput ja näin ollen etsiä mahdollisia ratkaisuja verkkoliikenteen jakautumiseen tasaisemmin.

Verkossa olevien palvelimien osalta Inspector pystyi näyttämään, mitä palveluja kyseisellä laitteella on käytössä. Lisäksi kunkin laitteen mahdolliset



Kuvio 3. Fluke Networks Network Inspector Console –pääikkuna

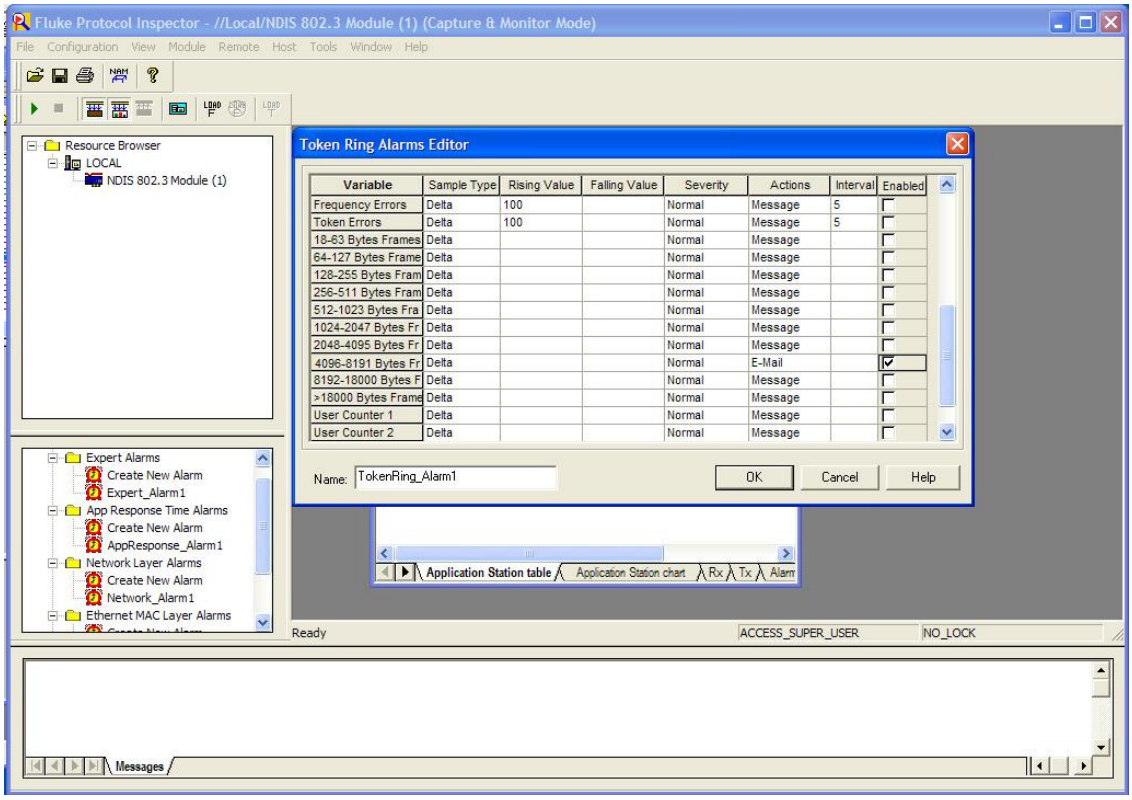
toimintavirheet tai muutokset toiminnassa näkyvät suoraan ns. laitekortissa, joka aukeaa kaksoisklikattaessa kyseistä laitetta pääikkunassa.

Pääohjelmalla pystytään lisäksi luomaan verkkokarttoja, joissa näkyvät kaikki tietojen keräyksen aikana päällä olleet laitteet. Laitteet voidaan verkkokartoissa erotella esimerkiksi IP-osoitteiden avulla ja kartat pystytään myös tarpeen mukaan tulostamaan. Tämä helpottaa eri verkkosegmenteissä olevien laitteiden sijaintien määrittämistä sekä esimerkiksi väärin nimetyn laitteen etsimistä, koska kartoista pystytään paikallistamaan laite helposti ja näin mahdollinen ongelma saadaan ratkaistua.

4.2.1 Hälytykset

Kaikki tarkempi verkon tutkinta sekä hälytyksien luominen tapahtui pääohjelmaan asetetun apuohjelman, Protocol Inspectorin, avulla. Protocol Inspector on verkon tarkkailun kannalta oleellisin osa koko ohjelmistoa, sillä

se sisältää niin datapakettien kaappaamisen, tilastojen luomisen kuin hälytysten luomisen.



Kuvio 4. Hälytysten laatiminen Network Inspectorissa

Protocol Inspectorin avulla voidaan luoda yksityiskohtaisia hälytyksiä. Oikean tyyppisen hälytyksen luominen osoittautui varsin haasteelliseksi ohjelmassa, sillä hälytyksiä voitiin luoda esimerkiksi verkkokerroksen tarkkailuun tai ohjelmarajapinnan tarkkailuun. Kun oikea vaihtoehto löytyi oli hälytyksen luominen helppoa. Ohjelmassa tulee määrittää vain kyseisen arvon muutoksen suunta, mahdollinen esiintymistiheys sekä toiminto, minkä ohjelma suorittaa hälytyksen sattuessa (Kuvio 4.). Ilmoituskeinoina olivat viesti sähköpostiin, hakulaitteeseen tai suoraan hallintapäätteelle.

4.2.2 Datapaketit

Datapakettien kaappauksen aloittaminen oli ohjelmassa helppoa. Mikäli minkäänlaisia hälytyksiä ei haluttu asettaa toimintaan, tarvitsi vain käynnistää

datan kaappaus. Kuten kaikissa testatuissa ohjelmissa myös Protocol Inspectorissa datapakettien sisällön tutkiminen oli todella hankalaa.

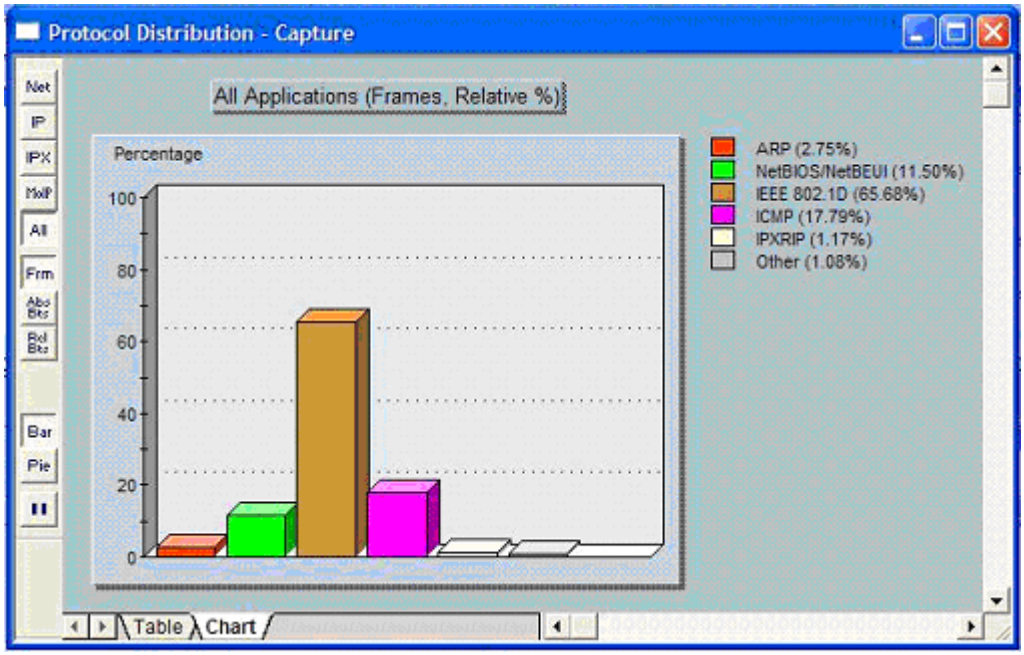
Mikäli datapaketti sisälsi tekstiä, pystyi sen ohjelman kautta lukemaan. Kaikki muu testauksessa liikuteltu data, kuten video- ja musiikkileikkeet, jäivät verkkoliikenteestä tunnistamatta. Ainoa tunnistettu muu kuin tekstiä sisältävä datapaketti oli eräs videoleike, jonka tunnisti kaapatusta datasta vain tiedostonimen perusteella.

Vaikkakin Protocol Inspector on kaikkein tarkin testatuista ohjelmista datapakettien kaappaamisessa ja tutkimisessa, on se myös epäselvin. Vaikka paketit näkyvät kuten muissakin testatuissa ohjelmissa listauksena, on erona muihin käyttäjän kannalta katsottuna tarkka tiedonanti liikkuvasta datasta. Tämä tarkoittaa sitä, että verkonvalvojan tulee olla hyvät pohjatiedot verkkoliikenteen perusteista ja datapakettien koostumuksesta.

4.2.3 Tilastot ja raportit

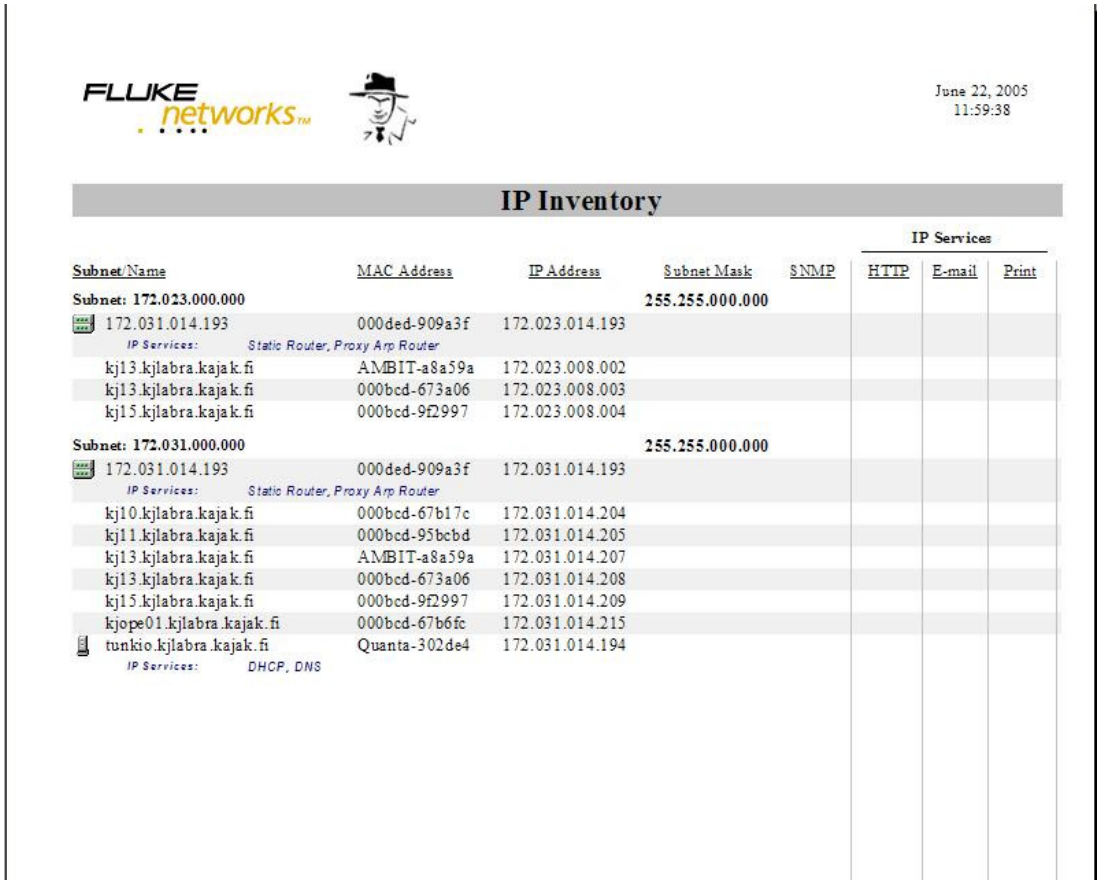
Ohjelma sisältää useita erilaisia tilastoja lähes kaikesta mistä niitä voidaan luoda verkkoliikennettä seurattaessa. Protocol Inspectorin tilastot antoivat kaikkein tarkinta tietoa verkon käyttöasteesta, datapakettien koosta sekä käytetyistä protokollista.

Graafit pystyttiin luomaan joko pylväs- tai piirakkamuotoon. Niiden avulla pystyttiin esimerkiksi tarkkailemaan laitteiden käyttämien protokollien osuuksia sen hetkisessä verkkoliikenteessä (Kuvio 5.). Lisäksi pystyttiin tarkastelemaan mitkä koneet vaihtoivat keskenään dataa ja mitkä koneet olivat yhteydessä Internetiin. Kahden koneen välisen tiedonsiirron määriä pystyttiin näin tarkkailemaan. Tämä voi olla avuksi esimerkiksi tilanteissa, joissa verkosta etsitään laitteita tai käyttäjiä, jotka siirtävät suuria määriä dataa keskenään tai lähiverkosta ulkomaailmaan esimerkiksi vertaisverkkojen kautta.



Kuvio 5. Pylväsgraafi testausympäristön laitteiden käyttämistä protokollista

Raportointiin on Network Inspectorissa useampia vaihtoehtoja. Ohjelmalla voidaan joko listata kaikki laitteet IP-osoitteen tai MAC-osoitteen mukaiseen järjestykseen ja näin ollen saadaan esimerkiksi tarkka kuva käytössä olevista IP-osoitteista (Kuvio 6.). Lisäksi raportteja voidaan laatia esimerkiksi virheilmoituksista tai trenditilastojen pohjalta.



June 22, 2005
11:59:38

IP Inventory

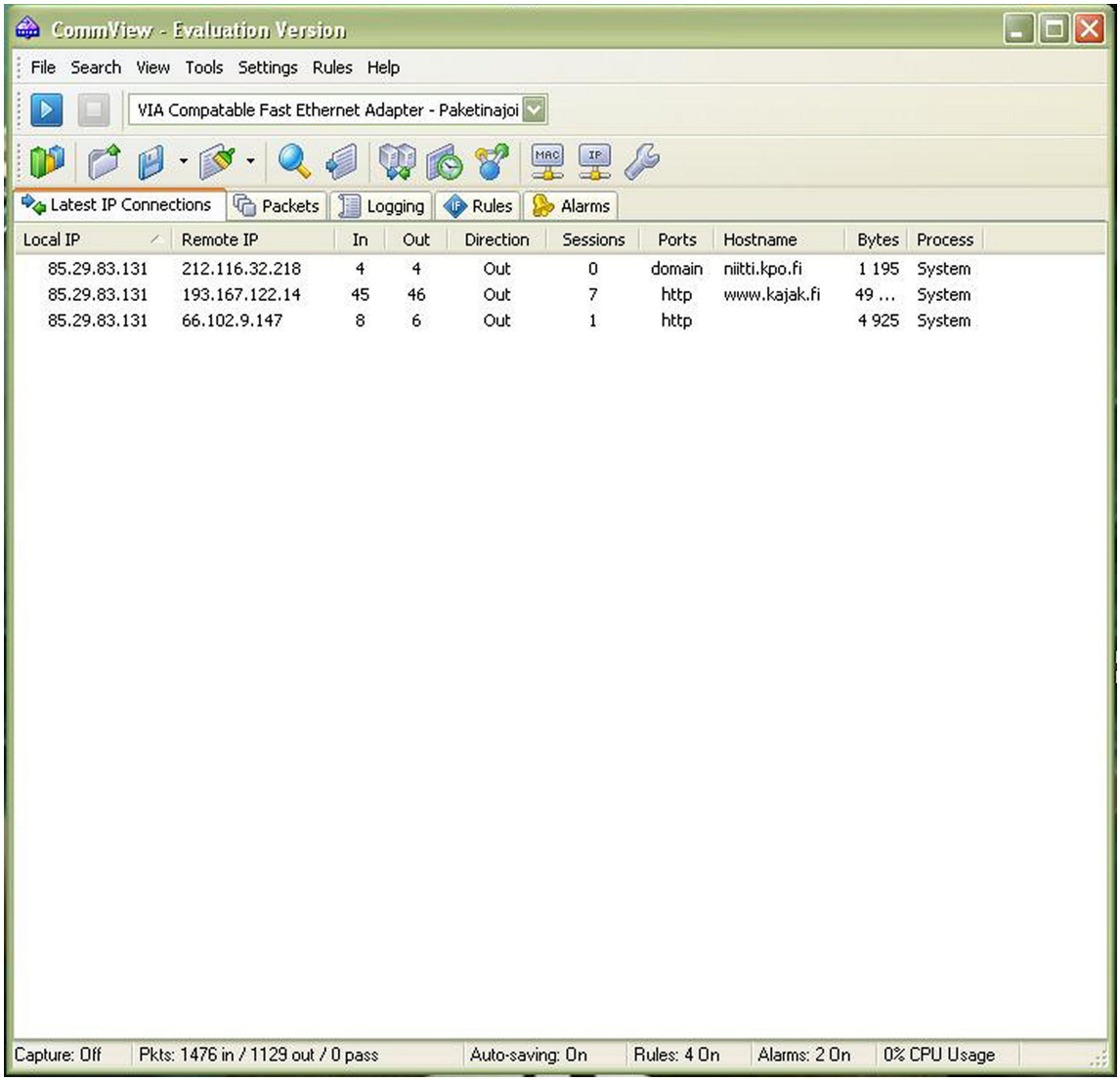
Subnet/Name	MAC Address	IP Address	Subnet Mask	SNMP	IP Services: HTTP	IP Services: E-mail	IP Services: Print
Subnet: 172.023.000.000			**255.255.000.000**				
172.031.014.193	000ded-909a3f	172.023.014.193					
IP Services: Static Router, Proxy Arp Router							
kj13.kjlabra.kajak.fi	AMBIT-a8a59a	172.023.008.002					
kj13.kjlabra.kajak.fi	000bcd-673a06	172.023.008.003					
kj15.kjlabra.kajak.fi	000bcd-9f2997	172.023.008.004					
Subnet: 172.031.000.000			**255.255.000.000**				
172.031.014.193	000ded-909a3f	172.031.014.193					
IP Services: Static Router, Proxy Arp Router							
kj10.kjlabra.kajak.fi	000bcd-67b17c	172.031.014.204					
kj11.kjlabra.kajak.fi	000bcd-95bcbd	172.031.014.205					
kj13.kjlabra.kajak.fi	AMBIT-a8a59a	172.031.014.207					
kj13.kjlabra.kajak.fi	000bcd-673a06	172.031.014.208					
kj15.kjlabra.kajak.fi	000bcd-9f2997	172.031.014.209					
kjope01.kjlabra.kajak.fi	000bcd-67b6fc	172.031.014.215					
tunkio.kjlabra.kajak.fi	Quanta-302de4	172.031.014.194					
IP Services: DHCP, DNS							

Kuvio 6. IP-inventaario Network Inspectorilla

4.3 Commview 5.0

Tamosoft:n kehittämä Commview 5.0 on maksullinen verkontarkkailuun tarkoitettu ohjelma. Se on toiminnaltaan ja käyttöliittymältään samankaltainen kuin Network Inspector. Commview:n etuna Network Inspectoriin verrattuna on selkeämpi käyttöliittymä sekä erilaisten ominaisuuksien suora esilläolo.

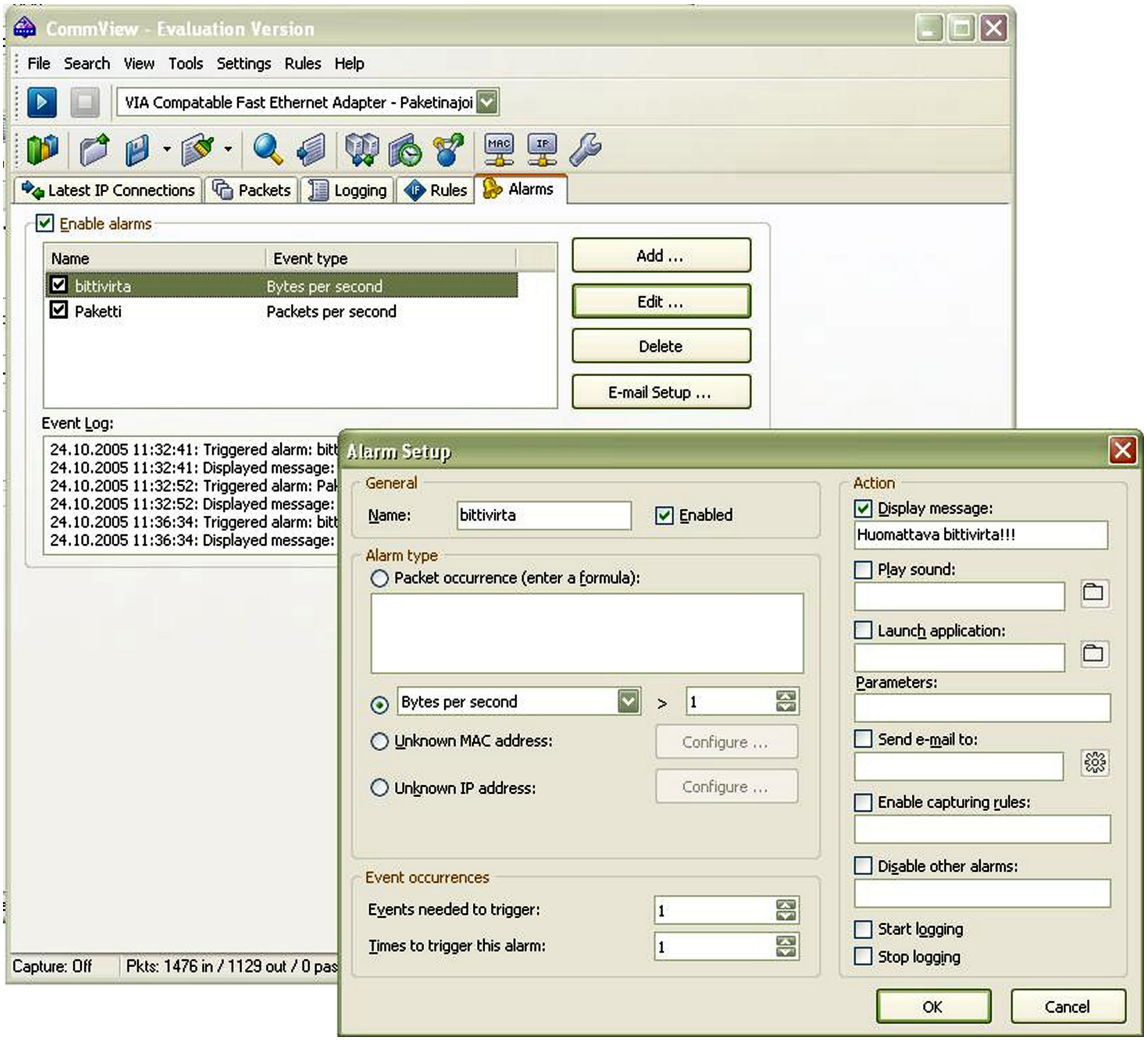
Erona Network Inspectoriin on se, ettei erillistä agenttiohjelmaa ole, vaan laite tutkii suoraan käynnistyttyään verkkolaitteen läpi kulkevaa dataa (Kuvio 7.). Näin ollen ohjelma tulisi asentaa pieniin lähiverkkoihin, joissa on keskuskone verkkoliikenteen jakamiseen.



Kuvio 7. Commview 5.0 pääikkuna

4.3.1 Hälytykset

Hälytyksien luominen Commview:ssä on huomattavasti helpompaa kuin Network Inspectorissa. Ensimmäinen tekijä helppouteen on, että ei tarvitse avata erikseen uutta apuohjelmaa, että hälytyksiä voi tehdä, sillä ne löytyvät suoraan hälytys-välilehden alta. Toinen tekijä on selkeämmät hälytysmallit, joihin voidaan antaa omat arvot, joiden täyttyessä tai joiden alittuessa hälytys annetaan.



Kuvio 8. Hälytysten luominen Commview:ssä

Ohjelmassa voidaan valita joko kaavamuotoinen hälytystyyppi, tai valita kolmesta valmiiksi olemassa olevasta vaihtoehdosta, joita ovat virheilmoitus bittivirran rajan ylityksestä, tuntematon MAC-osoite ja tuntematon IP-osoite. Kullekin luotavalle hälytykselle annetaan sitä kuvaava nimi ja lisäasetukset.

Hälytyksestä voidaan ilmoittaa muutamalla erilaisella tavalla. Helpoin on hälytysviestin näyttäminen, jolloin hälytyksen sattuessa työpöydälle ponnahtaa ikkuna, jossa lukee itse määritelty hälytysteksti (Kuvio 8.). Toiseksi hälytykset voidaan eritellä erilaisten äänten perusteella. Kolmanneksi voidaan hälytyksen tapahtuessa käynnistää ohjelma ja antaa sille jokin parametri ja näin ilmoittaa hälytyksestä. Tällainen ohjelma voisi olla esimerkiksi komentokehotteen net

send-käsky, jolla voidaan lähettää viesti jollekin tietylle tietokoneelle tai toimialueella käyttäjälle ja näin informoida tapahtuneesta hälytyksestä.

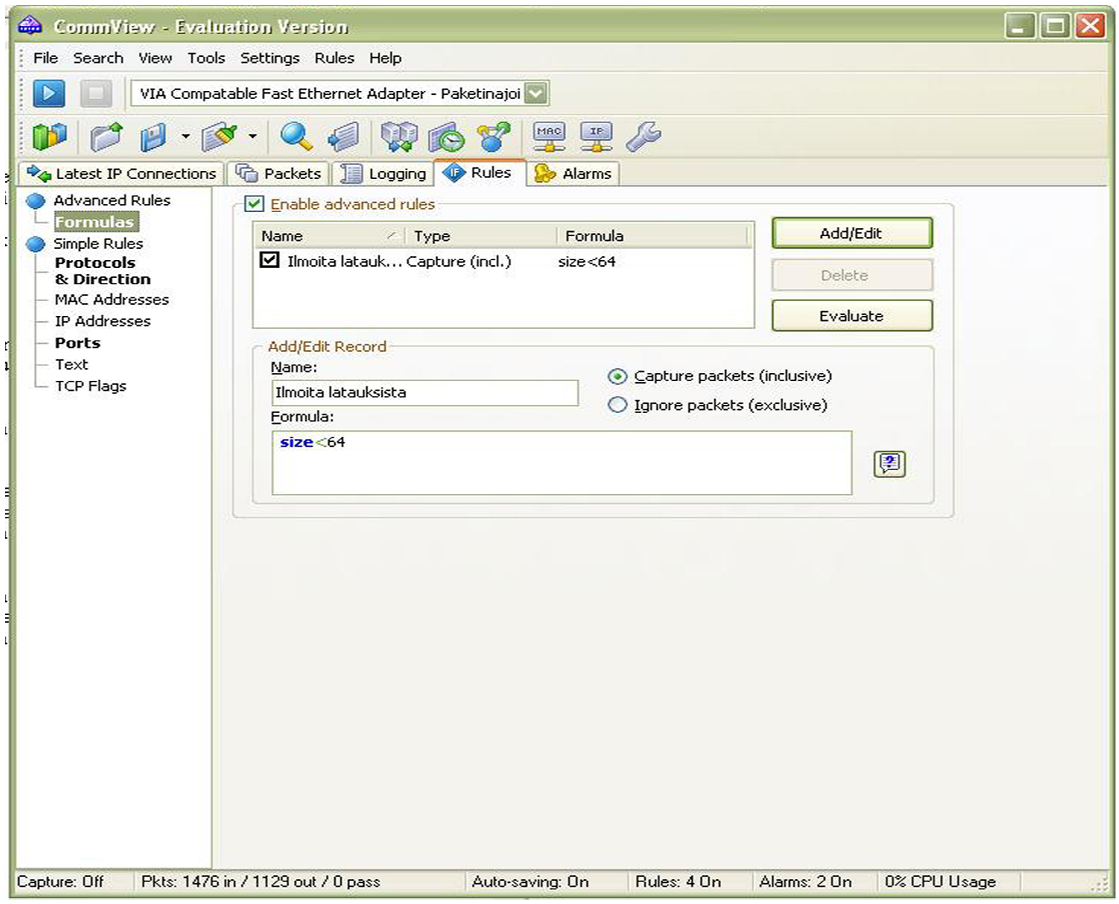
Mikäli ohjelma on käynnissä jollain muulla työasemalla kuin millä järjestelmänvalvoja työskentelee, voidaan hänelle lähettää sähköpostiviesti, josta käy ilmi hälytyksen syy. Näin järjestelmänvalvoja on aina tietoinen mitä hälytykset koskevat eikä hänen välttämättä tarvitse lähteä erikseen hallintapäätteelle katsomaan mistä on kyse.

4.3.2 Säännöt

Sääntöjen avulla voidaan rajata kaapattavan datan määrää ja laatua. Säännönlaatija voi valita, haluaako tehdä oman, tosi/epätosi-tyyppisen säännön, vai käyttääkö valmiita pohjia tai raja-arvoja, jotka ohjelma tarjoaa.

Säännöt voidaan laatia koskemaan protokollia, datapakettien liikettä, MAC-osoitteita, portteja, liikkuvaa tekstiä tai IP-osoitteita. Säännöillä saadaan rajattua tarkasti se, mitä verkosta halutaan kaapata tutkittavaksi. Lisäksi tämä mahdollistaa tietyn verkon solmun tutkimisen, esimerkiksi verkkohyökkäysten havaitsemisen ja verkon rasittuvuusasteen tilan.

Esimerkissä (Kuvio 9.) on laadittuna sääntö, jonka päällä ollessa kaapataan vain paketit, jotka ovat kooltaan alle 64 tavua. Säännön tuloksena kaapattavan datan määrä tippui, sillä näin pieniä datapaketteja liikkui verkossa testaushetkellä varsin vähän. Kuvassa näkyvät myös muut mahdolliset säännön luomiseen annetut tavat, kuten protokollat ja verkkoliikenteen suunta sekä portit ja MAC- ja IP-osoitteiden mukaiset säännöt. Näissä osoitteisiin perustuvissa säännöissä yksinkertaisesti annetaan raja-alue, jolta datapaketteja halutaan kaapata. Toiseksi voidaan antaa osoitteet, jotka jätetään tiedonkeruun ulkopuolelle.

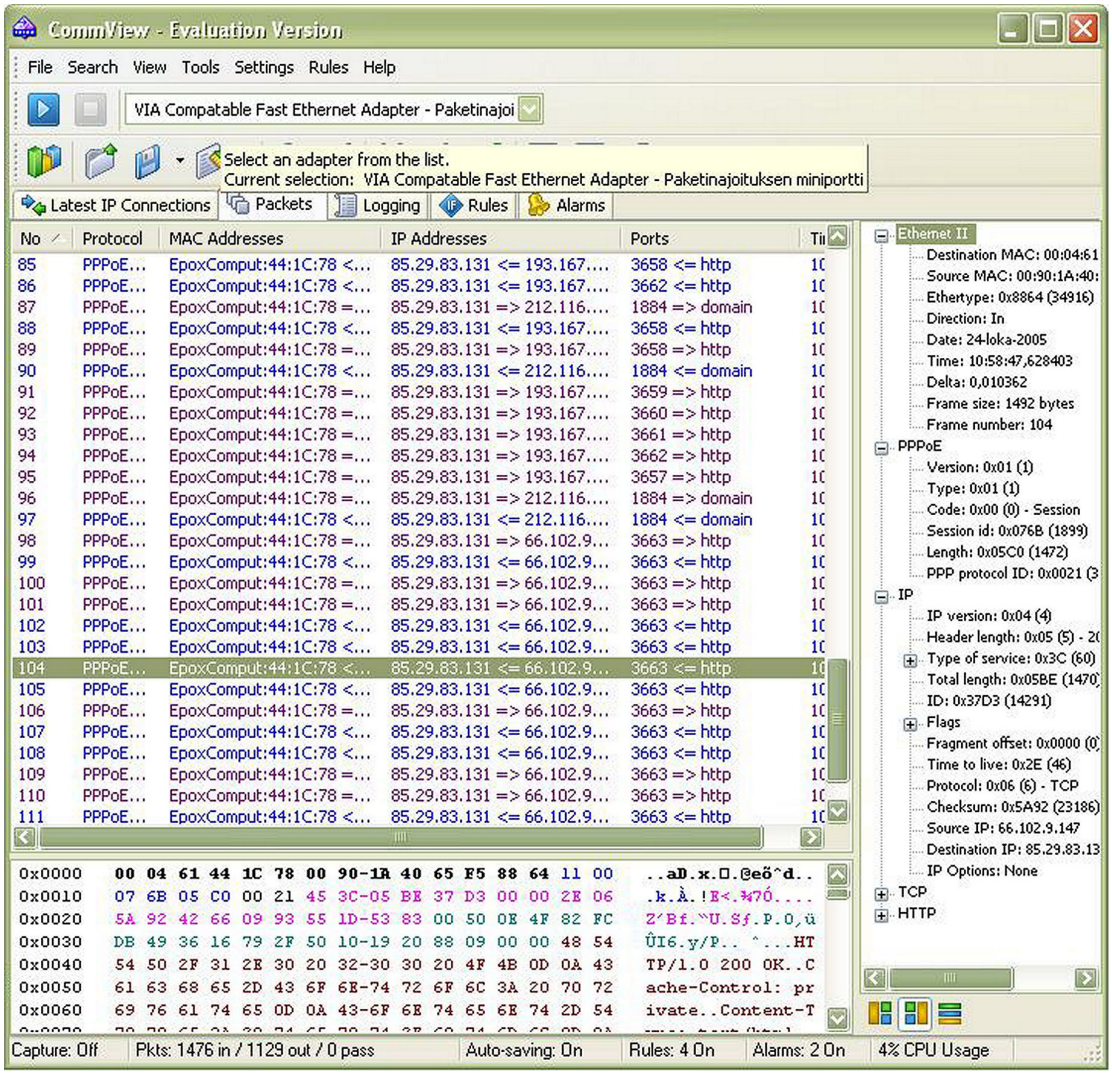


Kuvio 9. Sääntöjen laatiminen Commview:ssä

4.3.3 Datapaketit

Kaapatun datan sisällön tutkiminen on ohjelmassa haastavin tehtävä. Itse datapakettien keräys on helppoa, koska ei tarvitse tehdä muuta kuin käynnistää ohjelma ja kaikki liikkuvat datapaketit kirjautuvat ohjelman Packets-välilehdelle. Säännöillä voidaan rajata esitettävien datapakettien tyyppiä tai kokoa, mutta oletusarvoisesti kaikki paketit näkyvät listauksessa.

Verrattuna Network Inspectoriin on Commview:n datapakettien tutkiminen huomattavasti helpompaa. Ohjelma kerää ja esittää paljon informaatiota kyseisen datapaketin sisällöstä kuin liikesuunnastakin. Lisäksi ohjelma näyttää paketin kulkeman portin numeron sekä minkälaista verkkoliikennettä on ollut kyseessä (Kuvio 10.). Nämä tekijät helpottavat huomattavasti datapakettien tarkkailua ja etenkin niiden tarkoituksen selvittämistä osana verkkoliikennettä.

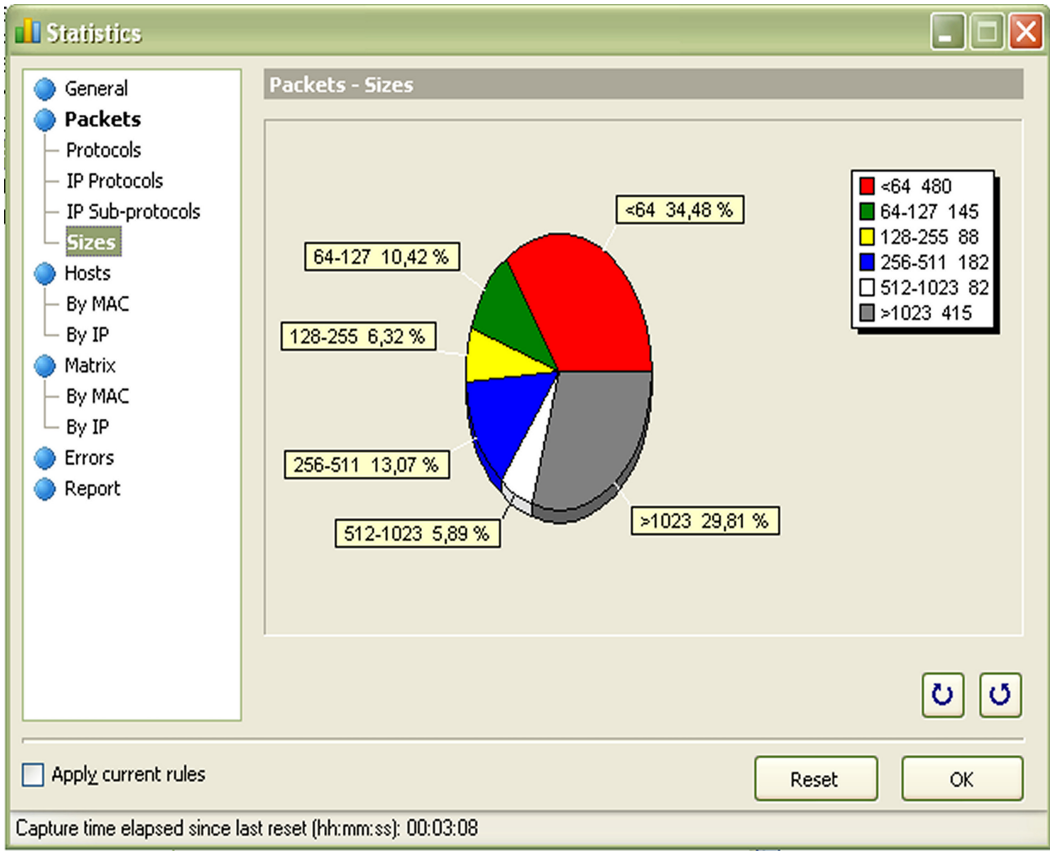


Kuvio 10. Kaapatun datan esittäminen Commview:ssä

Commview kerää datapaketteja vain sen työaseman verkkoliikenteestä, johon se on asennettuna, eli testausympäristössä se keräsi datapaketteja vain kannettavan tietokoneen verkkoliikenteestä. Testaustulokset ovat näin ollen vajavaisemmat verrattaessa Commview:tä ja Inspectoria. Useamman työaseman verkkoliikennettä olisi pystytty tarkkailemaan, mikäli kannettavan tietokoneen kautta olisi jaettu verkkoyhteys muille koneille.

4.3.4 Tilastot

Erilaisten tilastojen tarkastelu on Commview:ssä helppoa, koska kaikki tarjolla olevat tilastot löytyvät saman ikkunan sisältä. Tilastoja luodaan virheiden, laitteiden, tiedonsiirtoprotokollien sekä datapakettien kokojen mukaan.



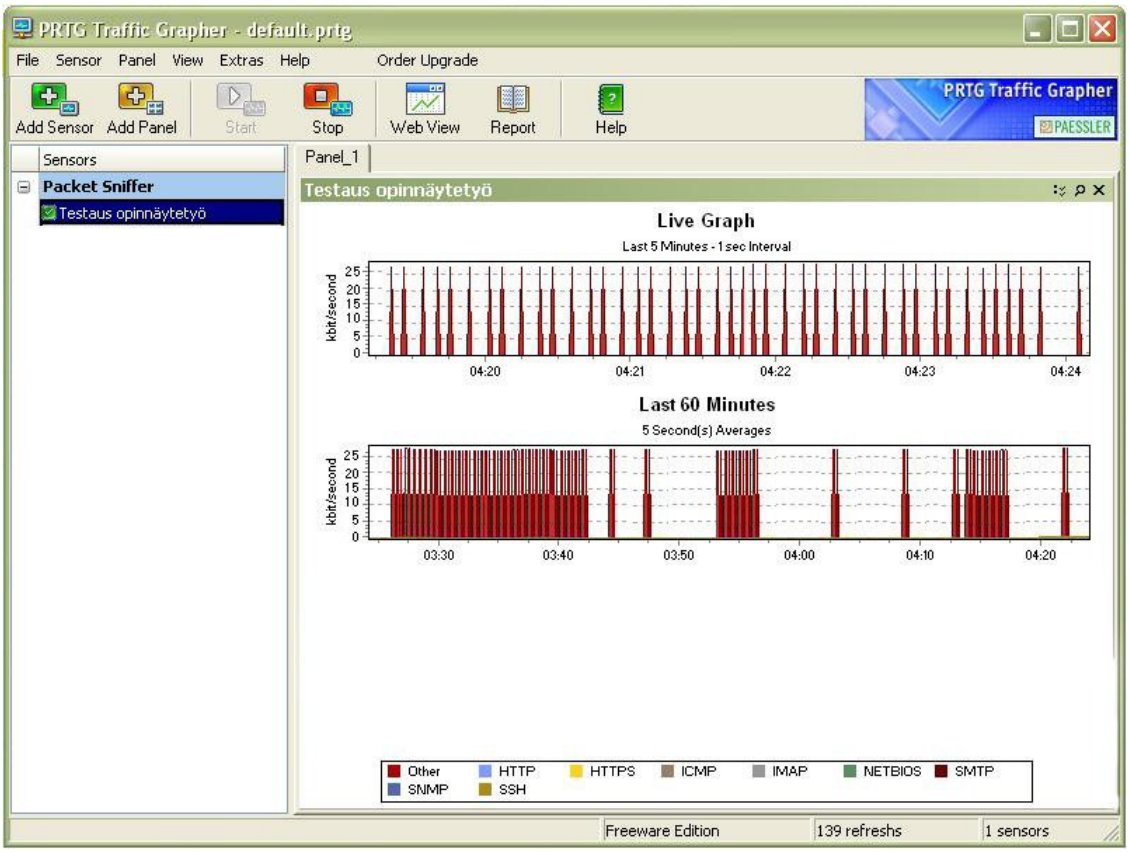
Kuvio 11. Tilasto pakettien koosta Commview:ssä

Erona Network Inspectoriin on selkeämpi ulkoasu sekä yksinkertaisemmat tilastot. Ottaen huomioon, että molemmat ohjelmat ovat maksullisia ja varsin tarkkoja toiminnassa, on Commview:n tilasto- ja raportointityökalut jätetty varsin pinnallisiksi verrattuna Network Inspectoriin (Kuvio 11.). Commview:n tilastot aukeavat helpommin myös hieman kokemattomammalle verkontarkkailijalle.

4.4 PRTG Traffic Grapher

PRTG Traffic Grapher on Paesslerin kehittämä verkkoliikenteen tarkkailuohjelma. Ohjelma on ilmainen, mutta siitä on olemassa myös maksullisia versioita.

PRTG Traffic Grapher on pienempiin verkkoihin tarkoitettu verkontarkkailuohjelma. PRTG:n etuna oli kaapatun datan tallentaminen sellaiseen muotoon, että sitä pystyvät muutkin analysointiohjelmat tutkimaan. Ohjelma on enemmän verkon käyttöasteen tarkkailua varten eikä näin ollen juuri muita tilastoja ole saatavilla kuin ajoittaisten verkon käyttöasteiden vertailu käyrädiagrammissa.



Kuvio 12. PRTG Traffic Grapher käyttöliittymä

PRTG ei kerää minkäänlaisia yksittäisiä laitetietoja, vaan se keskittyy vain verkkoliikenteen toiminnan laskelmointiin (Kuvio 12.). Ohjelmalla voidaan luoda kuva verkon käyttöasteesta jopa vuoden mittaisen tutkimustuloksen

pohjalta. Tätä ohjelmaa voisi käyttää lähinnä reitittimen liikenteen tarkkailuun ja laitteen kuormituksen seurantaan, koska ohjelmalla voidaan luoda käyrät erikseen ulospäin ja sisäänpäin menevälle liikenteelle ja näin seurata verkossa käytettäviä protokollia. Ohjelma tutkii liikennettä siitä laitteesta, johon se on asennettu, mutta se voidaan asentaa myös siten, että se tutkii tietyn IP-osoitteen läpi kulkevaa dataa. Tätä ei pystytty testaamaan, sillä ohjelman kokeiluversiolla tällaista määritystä ei voitu tehdä. Ohjelma eroaa näin ollen huomattavasti kahdesta muusta testatusta ohjelmasta, sillä muita toimenpiteitä ei juuri ohjelmassa ole tarjolla.

PRTG erottui joukosta vajavaisilla ominaisuuksillaan sekä varsin vaikeaselkoisella ulkoasullaan. Toisaalta PRTG kuvastaa sitä, kuinka erilaisia analysointiohjelmia on vapaasti ladattavissa käyttöön Internetistä.

4.5 YHTEENVETO

Verkonvalvonta ja verkkoliikenteen analysointi ovat toimintaa verkossa liikkuvan datan, verkon rasitusasteen ja muiden mittausten aikaansaamiseksi. Mittausten avulla saadaan kartoitettua mahdolliset verkon toimintaa hidastavat laitteet sekä tutkittua mitä ja millaista dataa verkossa liikkuu.

Lähes kaikki verkon analysointiohjelmat käyttävät SNMP-protokollaa tietojen keräämiseen verkkoliikenteestä. Se on yksinkertainen ja kevyt protokolla, joka on suunniteltu verkon liikenteen ja siellä olevien laitteiden tarkkailuun.

Yleisin toimintamalli verkon analysointiohjelmilla on hallintaohjelma/agentti-arkkitehtuuri. Tässä toimintamallissa agentti kerää heti käynnistämisestään alkaen erilaista tietoa verkon toiminnasta, joka pystytään analysoimaan hallintaohjelman avulla.

RMON-standardia sekä MIB-tietokantaa käytetään apuna niin agentin kuin hallintaohjelman suorittamien ilmoitusten tai hälytysten raja-arvojen luomisessa.

Verkon analysointiohjelmia löytyy paljon ja ominaisuuksiltaan paljon toisistaan erottuvia. Ilmaisohjelmista löytyy lähes vastaavia ohjelmia kuin tuotekehityksen tuloksena syntyneistä maksullisista ohjelmistoista. Tärkeintä on tietää, mitä haluaa ohjelmalla pystyttävän tekemään. Internet tarjoaa useita eri analysointitehtäviin erikoistuneita ohjelmia sekä kokonaisia verkonvalvontaohjelmistoja.

Testauksessa mukana olleiden verkon analysointiohjelmien ominaisuuksien erot olivat huomattavissa kahden ohjelman erottuessa edukseen kolmannesta (Taulukko 1.). Maksulliset ohjelmat sisälsivät huomattavasti ilmaista ohjelmaa laajemmat mahdollisuudet verkon tarkkailuun. Suuria eroja ei maksullisissa ohjelmissa ollut, mutta ominaisuuksien määrässä Network Inspector oli selkeästi muita edellä. Toisaalta laaja ominaisuuksien kirjo tarkoittaa sitä, että ohjelman käyttäjällä tulee olla hyvät perustiedot tietoverkoista sekä yleisesti tietoliikenteestä, että kaikki ominaisuudet saadaan hyötykäyttöön.

Ominaisuus	Network Inspector	Commview 5.0	PRTG Traffic Grapher
Laitetietojen keräys	+		
Hälytysten luonti	+	+	
Sääntöjen luonti		+	
Verkkoliikenteen kaappaus	+	+	
Tilastot	+	+	+
Raportointi	+		+
Verkkokartan luonti	+		

Taulukko 1. Ominaisuuksia ohjelmittain

Commview on hyvä ja selkeä verkon tarkkailuohjelma, jonka käyttäminen onnistuu varmasti hieman kokemattomammaltakin käyttäjältä pienen

ohjelmaan tutustumisen jälkeen. Selkeät valikot ja välilehdet sekä yksinkertainen tilastoikkuna ovat Commview:n parhaita puolia. Lisäksi ohjelmassa on varsin helppo luoda niin hälytyksiä kuin sääntöjäkin. Vaikka ohjelma ei ole aivan yhtä laaja kuin Network Inspector, on Commview huomioon otettava vaihtoehto, mikäli on kyse esimerkiksi pienen tai keskisuuren yrityksen verkon tarkkailusta. Helppokäyttöisenä, mutta kuitenkin tärkeimmät ominaisuudet sisältävänä ohjelmana, sen hallinnoinnin voi hoitaa pienemmissä lähiverkoissa periaatteessa kuka tahansa, jolle verkon tarkkailu on vastuulle annettu.

5 POHDINTA

Tämän opinnäytetyön tavoitteeksi asetettiin verkon analysointiohjelmiin tutustuminen ja Kajaanin ammattikorkeakoululla käytössä olevan analysointiohjelman vertailu muutamaan muuhun saatavilla olevaan ohjelmaan. Ohjelmien vertailu onnistui hyvin ja lopputuloksena saatiin kuva verkon analysointiohjelmien perustoiminnasta sekä vertailutulos ammattikorkeakoulussa käytössä olevaan ohjelmistoon.

Opinnäytetyössä tehdyn testauksen ja ominaisuuksien kartoituksen hyötyä ammattikorkeakoululle on vaikea arvioida, koska työn toteuttaminen on ollut lähes kokonaan opiskelijan vastuulla eikä ammattikorkeakoulun puolelta suuremmin oltu yhteydessä testauksen aikana sen suorittajaan. Mahdollinen hyöty opinnäytetyöstä ammattikorkeakoululle on sen käyttö apuna opetuksessa, mikäli verkon analysointia tullaan tulevaisuudessa tarkastelemaan jonkin opintokokonaisuuden osana. Enemmän hyötyä työstä sai kuitenkin testaaja tietotaidon kehittyessä lähes kokonaan uuden asian parissa.

Vertailu kolmen eri analysointiohjelman ominaisuuksista oli varsin helppoa, koska kaikki ohjelmat olivat samankaltaisia toiminnaltaan. Suurimpina eroina havaittiin monitorointitulokset ja kaappaustoimintojen erilaisuus. Jokaisessa vertailussa mukana olleista ohjelmista oli omat hyvät puolensa käyttäjän näkökulmasta katsottuna, mutta kokonaisuutena Fluke Networks Network Inspector oli paras ja ominaisuuksiltaan monipuolisin. Toisaalta ero

maksullisen ja ilmaisohjelman välillä tulee usein esille juuri ominaisuuksien määriä tutkittaessa.

Uuden tiedon määrä työtä tehdessä oli huomattava ja ohjelmiin tutustuminen mielenkiintoista puuhaa. Verkon analysoinnin vaikeus ja ohjelmien monipuolisuus yllättivät ja samalla lisäsivät halua oppia aiheesta lisää. Ohjelmien testaukseen aluksi varattu aika ei riittänyt kartoitukseen, jonka johdosta työn valmistuminen venyi yliajalle.

Opinnäytteen tekeminen kehitti työn tehneen opiskelijan verkonhallintataitoja, englanninkielistä asiasanaston osaamista sekä teorian sisäistämistä ja soveltamista käytännössä.

LÄHTEET

Cisco Ltd. 2005a. Saatavilla
http://www.cisco.com/univercd/cc/td/doc/cisintwk/
ito_doc/snmp.htm (Luettu 20.8.2005)

Cisco Ltd. 2005b. Saatavilla
http://www.cisco.com/univercd/cc/td/doc/cisintwk/
ito_doc/rmon.htm (Luettu 20.8.2005)

Niininen, K. 1997. Jyväskylän Yliopiston matematiikan laitos.
Ohjelmistotekniikan seminaari. Saatavilla
http://www.mit.jyu.fi/opiskelu/seminaarit/ohjelmistotekniikka/
openview (Luettu 9.9.2005)

Scott M. Ballew. 1998. IP-verkkojen hallinta. Erkki Suominen. Suomen ATK-kustannus Oy. Jyväskylä: Gummerus Kirjapaino Oy

The TCP/IP Guide. 2005. Saatavilla
http://www.tcpipguide.com/free/t_TCPIPNetworkManagementFra
meworkandProtocolsSNMPand.htm (Luettu 13.8.2005)

TCP/IP Trainer. 2005. Saatavilla
http://pww.evitech.fi/courses/mm2003/proj30/lapis/lapis/tcp%20ip/
tcpiptrainer-luku22.pdf (Luettu 4.11.2005)